UNIVERSITETET I OSLO
Institutt for informatikk

Infrastrukturbaserte 802.11 trådløse nett og 802.11i

Nettverksoppgradering og performance-evaluering

Masteroppgave

Kristian Svendsen

23. desember 2005

Sammendrag

IEEE 802.11i er en standard som spesifiserer sikkerhet i IEEE 802.11 trådløse nettverk. Denne oppgaven tar for seg oppgradering av infrastrukturbaserte 802.11 trådløse nettverk til 802.11i og ser på konsekvenser for brukeren. Throughput måles ved bruk av sikkerhetsmekanismen CCMP med standarden IEEE 802.1X for autentisering i stedet for WEP og forsøker å avdekke forskjeller i performance.

De involverte standarder gjennomgås, oppgradering til 802.11i forklares, throughput måles og oppgradering og resultatene diskuteres. Forslag til anvendelsesområder gis.

Oppgaven konkluderer med at CCMP benytter dobbelt så mange byte for å overføre informasjon nødvendig for sikkerhetsmekanismen som WEP, og at denne forskjellen i overhead lar seg måle selv for overføringer med store pakker.

Forord

Denne oppgaven, en kort masteroppgave, er skrevet som en del av min mastergrad i Informatikk ved Universitetet i Oslo, Institutt for Informatikk. Den er skrevet ved Universitetsstudiene på Kjeller (UniK) i perioden mandag 22. august 2005 til fredag 23. desember 2005. UniK har vært en meget hyggelig vert og har villig stilt utstyr til disposisjon for prøver og forsøk.

En takk går bl.a. til Frank Li og Anne Marie Hegland for kyndig veiledning, medstudentene Frode Mangseth og Øystein Heskestad for interessante diskusjoner rundt emnet og min familie som har utvist stor tålmodighet.

INNHOLDSFORTEGNELSE

FIGURLISTE

TABELLISTE

1 Terminologi

Dette kapittelet er inndelt i tre underkapitler Språk, Forkortelser og Definisjoner. Under Språk forklares foretatte språkvalg. Forkortelser som er benyttet i oppgaven finnes på fullstendig form under avsnittet om forkortelser. Definisjoner inneholder forklaring av noen ord og uttrykk som ikke er norske.

1.1 Språk

Denne rapporten er skrevet på norsk. Der en god norsk oversettelse av et engelsk ord eller uttrykk mangler, eller det av andre årsaker syntes mer hensiktsmessig å benytte den engelsk varianten er det gjort. Ordet eller begrepet er så forklart i kapittel ”1.3 Definisjoner”.

1.2 Forkortelser

802.11	IEEE 802.11
802.11i	IEEE 802.11i
802.1X	IEEE 802.1X
AES	Advances Encryption System
CA	Certificate Authority
CCMP	Counter Mode with CBC-MAC Protocol
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FCS	Frame Check Sequence
ICV	Integrity Check Value
IP	Internet Protocol
ISO	International Organization for Standardization
IV	Initial Vector
IEEE	Institute of Electrical and Electronics Engineers
MAC	Medium Access Control
MD5	Message Digest 5
MIC	Message Integrity Code
OSI	Open Systems Interconnection Reference Model, OSI referansemodell
POP	Post Office Protocol
PSK	Pre Shared Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RSN	Robust Security Network
SSID	Service Set Identifier
TKIP	Temporal Key Integrity Protocol

TSC	TKIP Sequence Counter
VoIP	Voice over IP
VPN	Virtuelt Privat Nettverk
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

1.3 Definisjoner

Nedenfor listes noen definisjoner.

Brukercredentialer:
Tegn som viser at en bruker er den han hevder å være, for eksempel brukernavn og passord.

Ethernet:
IEEE 802.3: standard for lokalnett.

IEEE 802.11:
Standard for trådløse lokalnett.

IEEE 802.11i:
Tillegg til 802.11 som definerer sikkerhet.

IEEE 802.1X:
Standard for portbasert tilgangskontroll.

”Security through obscurity”:
Sikkerhet ved hemmelighold av for eksempel metode eller implementasjon. Et eksempel fra dagliglivet kan være å gjemme nøkkelen under dørmatten.

2 Innledning

De senere årene har bruken av trådløse nettverk eksplodert, og det finnes snart trådløse nett hvor som helst. Fascinerende er det at til tross for tabloidpressens gjentatte oppslag om hvor farlig det er å ikke sikre sine trådløse nett, kan en som ønsker stoppe utenfor omtrent et hvilket som helst kontorbygg og koble seg til Internett.

2.1 Bakgrunn

Den hyppigst benyttede standarden for trådløse lokalnett er 802.11[2]. Standarden for sikkerhet i 802.11 trådløse har fått tittelen 802.11i[3]. Sikkerhetsmekanismen i 802.11 heter WEP. I 802.11i spesifiseres også TKIP og CCMP. En undersøkelse viser at av 706 trådløse knutepunkt funnet i Bergen, benyttet kun en drøy tredjedel kryptering[1].

Denne oppgaven vil omhandle 802.11i standarden, og ta for seg noe av det som skjer når et nettverk oppgraderes fra WEP til CCMP, altså erstatter WEP med CCMP samt autentiseringsmekanismen benyttet i 802.11i. Hvordan endring av sikkerhetsmekanisme i et trådløst lokalnett påvirker overføringen av IP-trafikk vil være en stor del av denne oppgaven. I tillegg vil det foretas en teoretisk diskusjon av hvordan den nye standarden for sikkerhet i trådløse lokalnett kan benyttes for å ta seg av både tilgangskontroll og konfidensialitet.

I oppgaven vil også Wi-Fi alliance, en sammenslutning av mange av de store industriselskapene som for eksempel 3Com, Cisco, Fujitsu-Siemens, Microsoft osv., nevnes. Organisasjonen sertifiserer produkter som ”Wi-Fi certified” når de tilfredsstiller kravene i 802.11 standardene og garanterer at produkter fra forskjellige produsenter fungerer sammen. Produkter basert på et tidlig utkast av 802.11i, som bare tilbyr TKIP utover WEP, kan få en WPA (Wi-Fi Protected Access) sertifisering og de som tilfredsstiller den endelige versjonen, og støtter CCMP, kan bli WPA2 sertifisert.

2.2 Mål, problemstilling og begrensninger

Mål:
Hovedtemaet i oppgaven vil være oppgradering av sikkerhet i IEEE 802.11 trådløse nett ved å ta i bruk 802.11i og endre sikkerhetsmekanisme fra WEP til CCMP. Målet med oppgaven er å evaluere performance med hensyn på sikkerhetsmekanismene WEP og CCMPs påvirkning av gjennomstrømningshastigheten (throughput) av IP-trafikk, vurdere hvordan brukeren kan føle endringen og gi et par eksempler der det bør vurderes å implementere 802.11i for å øke sikkerheten.

Problemstilling:
Hvordan kan et nettverk oppgraderes fra WEP til CCMP med 802.11is tilhørende autentiseringsmekanisme? I hvilken grad påvirkes gjennomstrømningshastigheten

(throughput) av IP-trafikk når WEP erstattes med CCMP for kryptering og 802.11is tilhørende autentiseringsmekanisme? Og i hvilken grad kan brukeren oppfatte at WEP erstattes med CCMP for kryptering og 802.11is tilhørende autentiseringsmekanisme?

Begrensninger:
I denne oppgaven vil målekriteriet for performance være throughput. Performance vil måles på nettverkslag.

2.3 Oversikt over oppgaven

Kapittel tre tar for seg sikkerhetsmekanismene som berøres i forbindelse med oppgradering til 802.11i. Først gis litt informasjon om nettverkssikkerhet.

Kapittel fire omtaler oppgradering til 802.11i og beskriver oppsett av testnettverk.

Kapittel fem tar for seg de testene som har vært utført for å finne ut hvordan performance påvirkes når testnettet benytter CCMP i forhold til WEP.

Kapittel seks diskuterer oppgradering til 802.11i, resultatene av testene og hvordan 802.11i kan anvendes.

Kapittel syv konkluderer og forslår videre arbeid.

3 Oversikt over sikkerhetsmekanismer i forbindelse med 802.11i

Denne delen av oppgaven er inndelt i kapitlene Nettverkssikkerhet, IEEE 802.11 og WEP, IEEE 802.11i/WPA2 og andre mekanismer. Underkapitlet Nettverkssikkerhet gir litt kort informasjon om temaet og etterfølges av informasjon om de standarder som berøres ved oppgradering til 802.11i og oppsett av testnett.

3.1 Nettverkssikkerhet

I arbeidet med nettverk er kommunikasjonen delt opp i forskjellige lag. På denne måten kan man arbeide med forskjellige teknologier omtrent uavhengig av hverandre, kun begrenset til å tenke på det standardiserte grensesnittet til laget over eller laget under. Det er vanlig å referere til OSI-modellen. OSI-modellen er en abstraksjon definert av ISO (International Organization for Standardization).

Tabell 1: OSI-modellen[4]

Lag:	Beskrivelse:	Overføringsenhet:
7	Applikasjon	Data
6	Presentasjon	Data
5	Sesjon	Data
4	Transport	Segment
3	Nettverk	Pakke
2	Datalink	Ramme
1	Fysisk	Bit

Sikkerhet kan innarbeides på alle nivåer i OSI-modellen. Eksempler på sikkerhetsmekanismer i noen av lagene er for lag 7 S/HTTP[5], lag 3 TLS[6], og for lag 2 WEP og CCMP. WEP og CCMP vil omtales senere.

Noen sikkerhetstrusler som kan oppstå i nettverk er:

- Uvedkommende kan få tilgang
- Uvedkommende kan få tilgang ved å utgi seg for å være en berettiget bruker
- Informasjon kan avlyttes, lagres og tolkes av uvedkommende, og kan for eksempel spilles av eller overføres på nytt i sin opprinnelige eller endret form
- En angriper kan drukne nettet med data, som fører til at nettet overbelastes eller at berettigede brukere nektes dets tjenester.
- Uvedkommende kan opptre som mellommenn, og overbevise en annen del av nettet, som for eksempel klienter, at de er en tjener eller knutepunkt

For å hindre at uvedkommende får tilgang til nettet kan det sikres fysisk eller med sikkerhetsmekanismer. Et trådbasert nettverk kan låses eller stenges inne, men det er ikke mulig å få til med et trådløst nettverk. For å sikre tilgang kun for legitime brukere kan vi

bruke tilgangskontroll-, autoriserings-, autentiserings- og identifikasjonssystemer. For at ikke andre innen rekkevidde av det trådløse nettet skal kunne avlytte trafikken bruker vi konfidensialitetsmekanismer. Dersom en angriper ønsker kan han forsøke å endre på trafikk underveis i en overføring, eller spille av samme melding om igjen. For å hindre dette kan vi benytte integritetsmekanismer.

Eksempler på noen av disse angrepene kan være at en angriper forsøker å modifisere en melding mellom en bruker og en nettbank for å omdirigere en pengeoverføring. En nettbank kan benytte kryptering på applikasjonslaget for å sikre en slik forbindelse. Et eksempel på kommunikasjon som vanligvis er avhengig av sikkerhet i underliggende lag er henting av e-post ved hjelp av en e-postklient. I mange tilfeller er protokollen som benyttes ikke sikret. Dersom en bruker for eksempel knytter seg til et trådløst nett uten sikkerhetsmekanismer kan alle innen rekkevidde avlytte kommunikasjonen, inkludert brukernavn og passord brukeren benytter for å hente e-post. Er nettverket sikret, men med en nøkkel som deles av alle brukerne, har alle som har tilgang til nøkkelen tilgang til den informasjonen du overfører.

3.2 IEEE 802.11 og WEP

I juni 1997 ble IEEE standarden 802.11[2] utgitt. Det er en standard for trådløs kommunikasjon som etter hvert er blitt svært populær og utbredt. Den spesifiserer overføring via infrarøde signaler (IR) og i 2,4GHz ulisensiert radiobånd til industrielle, vitenskapelige og medisinske formål. Dette fører til at brukere kan oppleve forstyrrelser fra for eksempel mikrobølgeovner og trådløse telefoner. Infrarød har i praksis ingen anvendelse i trådløse nett.

802.11 omfatter datalinklaget og det fysiske laget i OSI modellen[4]. Standarden deler trådløse nett i to hoveddeler: Infrastrukturbaserte og Ad-Hoc nett. En celle, eller Basic Service Set, er en gruppe maskiner som kommuniserer med hverandre direkte (Independent BSS) eller gjennom et knutepunkt (Infrastrukturbasert BSS). Når flere knutepunkt koblet sammen utgjør et trådløst nettverk kalles dette Extended Service Set (ESS).

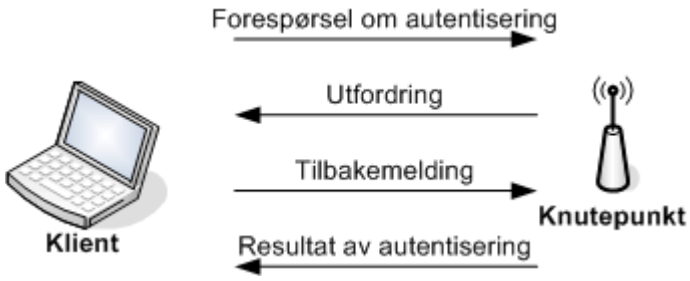
802.11 standarden videreutvikles kontinuerlig gjennom arbeidsgrupper i IEEE som forbedrer og legger til funksjonalitet. Tabell 2 lister noen av tilleggene til den opprinnelige standarden.

Tabell 2: Noen tillegg til standarden IEEE 802.11

Tillegg:	**Funksjon:**
802.11a	Muliggjør overføringshastigheter på 54Mbps. Benytter 5GHz båndet
802.11b	Benytter fremdeles 2,4GHz båndet, men muliggjør overføringshastigheter på 11Mbps
802.11c	Definerer bridge muligheter.
802.11e	Introduserer støtte for tjenestekvalitet og multimediestøtte
802.11g	Benytter 2,4GHz båndet for overføringshastigheter opptil 54Mbps.
802.11i	Spesifiserer sikkerhet

802.11 standarden definerte tre typer autentisering: Åpen autentisering (open system), delt nøkkel-autentisering (shared key) og høyere lag-autentisering (upper layer). Åpen autentisering er egentlig ikke autentisering i det hele tatt. Man stoler på alle. Meldinger om identitet og om man aksepterer autentiseringen utveksles.

Delt nøkkel-autentisering tar mål av seg til kun å autentisere de stasjonene som kjenner en felles nøkkel. Nøkkelen partene deler utveksles ikke som en del av autentiseringen, men i en egen prosess. Den er kjent fra før. Autentiseringen foregår ved at en utfordring genereres og overføres til klienten. Klienten krypterer utfordringen og sender den tilbake. Dersom knutepunktet kan dekryptere tilbakemeldingen og få ut den opprinnelige utfordringen kan det anta at de har samme nøkkel. Autentiseringen er vellykket og stasjonen er autentisert. Figur 1 viser fremgangsmåten. Autentiseringen er sårbar for avlytting, i det en som lytter på forbindelsen vil være i stand til senere å autentisere seg med samme identifikasjon ovenfor knutepunktet som klienten den avlyttet.



Figur 1: Autentisering ved hjelp av utfordring og tilbakemelding

En annen ulempe er at dette er enveisautentisering. Når det er kun klienten som autentiserer seg overfor knutepunktet har klienten ingen forsikring om at knutepunktet han kobler seg til er legitimt. Knutepunkt kan være satte opp ved en feiltakelse eller med hensikt, både av personer med gode hensikter og kjeltringer. En person med onde hensikter kan for eksempel utnytte dette for å avlytte kommunikasjon på jakt etter informasjon som kan utnyttes, eller han kan opptre som mellommann og forsøke seg på å forfalske informasjon.

I den opprinnelige 802.11 standarden av 1997 var behovet for konfidensialitet forsøkt dekket ved hjelp av ”Wired Equivalent Privacy” algoritmen, forkortet WEP, basert på RC4. Dette er også den krypteringen som benyttes under autentisering, som omtalt ovenfor. I trådbundne nettverk, for eksempel 802.3 standarden for Ethernet, er det ikke vanlig å tenke lenger på konfidensialitet enn å sikre kontroll over kabelen. Når overføringsmediet blir trådløst har vi ikke lenger kontroll på hvor dataene tar veien, og må tenke nøyere gjennom hvordan vi sikrer de mot avlesning av en uønsket tredjepart. WEP ble laget for å sørge for samme grad av sikkerhet som i et trådbasert nett. Dette er kanskje en grunn til at det ikke ble investert mye ressurser på dette området.

WEP består av en krypteringsalgoritme kalt RC4 og en protokoll for integritetsbeskyttelse (Integrity Check Value; ICV) basert på CRC-32[9]. Opprinnelig var det kun mulig å benytte 40 bits lange nøkler. Allerede i 1997 var dette for kort. Årsaken til valg av så korte nøkler var at det ikke var tillatt å eksportere lengre nøkler til land utenfor USA og Canada. Senere, da det amerikanske handelsdepartementet hevet restriksjonene, ble nøkkellengden økt til 104 bit. Disse refereres ofte til som 64-bits og 128-bits WEP-kryptering. Her er det nødvendig å være klar over at nøklene er 40 og 104 bits lange. De siste 24 bitene (4 byte) er initialvektoren (IV-en)

De alvorligste svakhetene til WEP er
• ICV-algoritmen

• Nøkkelhåndtering/initialisering
• Gjenspilling (replay)
• RC4s ”svake nøkler”

ICV-algoritmen er lineær og basert på en enkel sjekksum (CRC). Den krypteres sammen med meldingen. Sjekksummer er ikke kryptografisk sikre, og det er mulig å enkelt regne seg frem til hvilken verdi den skal ha. Dette innebærer at dersom den krypterte informasjonen endres er det ingen kunst å oppdatere sjekksummen uten at det detekteres ved dekkryptering.

I standarden er det ikke definert noen form for nøkkelhåndteringen. WEP overlater all nøkkelhåndteringen til utstyrprodusenten. Ikke mange implementerte noen mekanisme for dette. Manuell administrasjon og distribusjon av nøkler er meget krevende. Oftest benyttes gruppenøkler, og ikke parvise nøkler[10]. Når nye nøkler skal distribueres må alle motta og ta i bruk nøkkelen på samme tid, ellers mister de kontakt med knutepunktet. Når er person ikke lenger skal ha tilgang til nøkkelen må den byttes. Dette krevende regime fører som oftest til at nøkler sjelden byttes.

Initialiseringsvektoren (IV-en) er på 24 bit og sendes åpent i hver pakke. Hver pakke som overføres får ny IV. 2^24 gir litt få muligheter. Dette fører til at IV-ene alt for raskt gjenbrukes. Et travelt knutepunkt kan gjennomløpe et sett med IV-er på 24 bit i løpet av en time[7]. En angriper kan se når en IV gjenbrukes, og siden nøkler som oppdateres manuelt sjelden endres gir dette dårlig sikkerhet. For optimal sikkerhet med et flytchiffer som RC4 må IV aldri gjenbrukes, eller nøkkelen byttes før IVen benyttes igjen. En angriper som har samlet flere pakker med samme IV og nøkkel kan regne ut nøkkelen. (Sammen med kjente faste felter i en pakke avslører svake IV-er nøkkelen[12])

WEP gir ingen beskyttelse mot at en angriper kan spille av gamle pakker om igjen (replay).

RC4 har også et stort antall ”svake nøkler” som gjør det lettere å kryptanalysere data kryptert under disse nøklene[12]. Dette forenkler arbeidet til angriperen betraktelig dersom de blir brukt. Det er vanskelig å unngå disse siden det ikke er spesifisert noen nøkkelhåndteringsmekanismer.

Til tross for at WEPs svakheter er det bedre å benytte en dårlig sikkerhetsmekanisme enn ingenting. Ytterligere tiltak er nødvendig for å oppnå et tilfredsstillende sikkerhetsnivå. For å bøte på manglende sikkerhet i WEP er VPN en løsning som er flittig brukt. En VPN løsning kan også sikre kommunikasjonen lenger ut i nettet enn bare til knutepunktet. Derimot kompliserer en VPN løsning siden det er behov for en VPN-gateway. Ved å sikre datalinklaget vil også for eksempel ARP- og Ethernetrammer sikres, ikke bare IP-rammer.

3.3 IEEE 802.11i/WPA2

IEEE ble tidlig klar over svakhetene i 802.11s WEP. Arbeidet med et tillegg til standarden startet i 2001. Arbeidsgruppen het arbeidsgruppe ”i”, og tillegget fikk navnet 802.11i. Tillegget ble ferdigstilt i 2004.

I mellomtiden syntes ”Wi-Fi alliance” arbeidet tok lenger tid enn hensiktsmessig for virksomheten til alliansens medlemmer, og de bestemte seg for at de ville lage en midlertidig

løsning frem til tillegget ble ferdig. De gav produkter som tilfredstilte et tidlig utkast av standarden WiFi Protected Access (WPA)-sertifisering. WPA benytter seg av Temporal Key Integrity Protocol – TKIP) som kan sies å være en utvidelse av WEP. TKIP er en midlertidig løsning som retter opp noen feil og forbedrer WEP, og som i den endelig standarden er med for bakoverkompatibilitet med tidligere produsert maskinvare. TKIP kan kjøre på samme maskinvare som WEP. WPA har forbedret nøkkelhåndtering, initialisering og støtter ikke kortere nøkler enn 128-bits samt forbedret integritetsbeskyttelse for å forhindre forfalskning av meldinger og gjenspilling (replay).

I TKIP er lengden på initialiseringsvektoren doblet, ved at en utvidet 4 bytes IV legges til den opprinnelig IVen og den er omdøpt til TKIP Sequence Counter (TSC). Siden TSC oppdateres for hver pakke kan 2^48 pakker utveksles før antall IV-er blir oppbrukt, og den midlertidige nøkkelen må skiftes. Dette ville tatt mange år. TSC benyttes også til beskyttelse mot gjenspillingsangrep. En mottaker skulle forkaste pakker som er utenfor rekkefølge. Det er også implementert en funksjon for å eliminere svake IV-er. Som integritetsbeskyttelse benyttes ”MIChael”[13]. MICen er implementert som en enveis hash-funksjon, i motsetning til en CRC som danner grunnlag for WEPs ICV. Dersom MIC feiler forkastes meldingen. Deretter iverksettes tiltak, inkludert ny nøkkelutveksling og logging.

Under arbeidet med 802.11i var det foreslått å benytte seg av en eksisterende standard 802.1X[8] til autentisering og nøkkelhåndtering. Denne standarden benytter seg igjen av RADIUS[18] (Remote Authentication Dial-In Service). Ettersom man innså at det kanskje var for mye å forlange at alle hjemmebrukere skulle måtte sette sine egne Radiusservere, ble det også implementert en variant med forhåndsdelt nøkkel PSK, der PSK står for Pre-Shared Key. Her lager man en 256-bits nøkkel (en forhåndsdelt nøkkel) som man deler ut til alle som skal ha tilgang til knutepunktet. PSK brukes som et utgangspunkt for å lage en unik 128-bits nøkkel for hver klient. Det er vanskelig og lite brukervennlig å huske 64 vilkårlige heksadesimale siffer i hodet, så det ble lagt inn en mulighet for å spesifisere PSK som et passord på minst 8 tegn. Ulempen med dette er at for eksempel et passord på 32 tegn som konverteres til 256 bit ikke gir 256 bits sikkerhet. Brukes PSK med for korte passord, er det mulig å gjennomføre vellykkede forsøk på ordlistebasert passordknekking. Standardens[3] Annex H4 antyder at passord med kortere tegnlengde enn 20 vanskelig kan stå imot et angrep.

802.1X løser problemene med autentisering i WEP, og manglende nøkkelhåndtering. Autentiseringen kan foretas med hvilken som helst EAP[17]-basert metode. EAP omtales senere. Nøkkelhåndteringen er sentralisert, og tildeler parvise nøkler. Den har også en mekanisme for å endre og distribuere gruppenøkler. Fra 802.1X hentes følgende funksjoner eller mekanismer:

- En 802.1X Port[8] som ligger over MAC, slik at all trafikk som går gjennom MAC også går gjennom 802.1X porten. 802.1X benytter seg av autentisering på høyere nivå, og bidrar også med nøkkelhåndtering. Dette konseptet vil forklares nærmere i kapittelet om 802.1X.
- En ”Authenitication Agent”. Denne finner vi rett over 802.1X porten. Den bidrar med autentisering og nøkkelhåndtering. Dette vil også forklares nærmere i kapittelet om 802.1X.
- En ”Authentication Server”. Denne tjeneren bidrar med det som er nødvendig for å autentisere stasjonene i nettet. RADIUS er et eksempel på en slik tjener, og omtales nærmere i kapittelet om RADIUS.

802.11i-standarden definerer to kategorier rammeverk for sikkerhet. Robust Security Network (RSN) og pre-RSN. Et "Robust Security Network" støtter høyere lag-autentisering basert på 802.1X og har følgende karakteristikker[27]:

- Gjensidig autentisering av knutepunkt og stasjoner
- Nøkkelhåndteringsalgoritmer
- Etablering av kryptografiske nøkler
- Mekanisme for integritetsbeskyttelse og konfidensialitet, Counter Mode/CBC-MAC protocol (CCMP)

Når et trådløst nettverk oppgraderes til 802.11i benyttes Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) for å oppnå Robust Security Network (RSN). CCMP baserer seg på AES-kryptering (Advanced Encryption Standard)[14], og var utviklet for IEEE 802.11i. Counter Mode (CM) delen av CCMP er datakonfidensialitetsmekanismen, mens Cipher Block Chaining Message Authentication Code (CBC-MAC) står for dataintegritetsbeskyttelse og autentisering. CCMP er krevende for maskinvaren, og gammelt utstyr må skiftes ut. Den utbedrer alle WEPs kjente svakheter ved å forebygge endring av rammene av uvedkommende og forsøk på gjenspilling, retter opp WEPs feilbruk av kryptering og gjenbruker ikke nøkler[15].

Tabell 3 oppsummerer og sammenligner de viktigste egenskapene ved WEP, TKIP(WPA) og CCMP(WPA2).

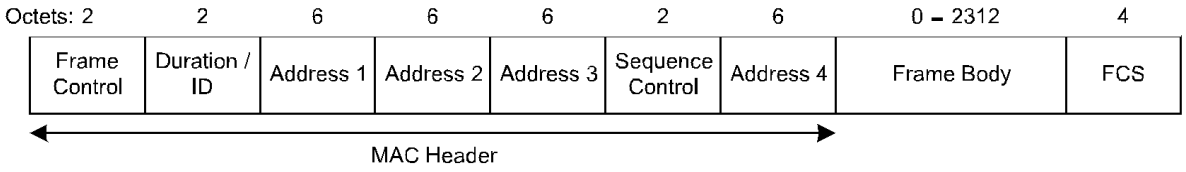
Tabell 3: Sammenligning av sikkerhetsfunksjoner i 802.11 trådløse nett[24]

	WEP	TKIP(WPA)	WPA2/802.11i
Chiffersystem	RC4	RC4	AES
Nøkkellengde	40 bit 104 bit	128 bit kryptering 64 bit autentisering	128 bit
IV-lengde	24 bit IV	48 bit IV	48 bit IV
Dataintegritets-beskyttelse	CRC-32	Michael	CCM
Rammehode-integritets-beskyttelse	Ingen	Michael	CCM
Gjenspillings-angrepsbeskyttelse	Ingen	IV-sekvens	IV-sekvens
Nøkkelhåndtering	Ingen	EAP-basert	EAP-basert

Formatet på MAC rammene spesifiseres i 802.11/802.11i standardens kapittel 7.1. Hver ramme består av følgende basiskomponenter:

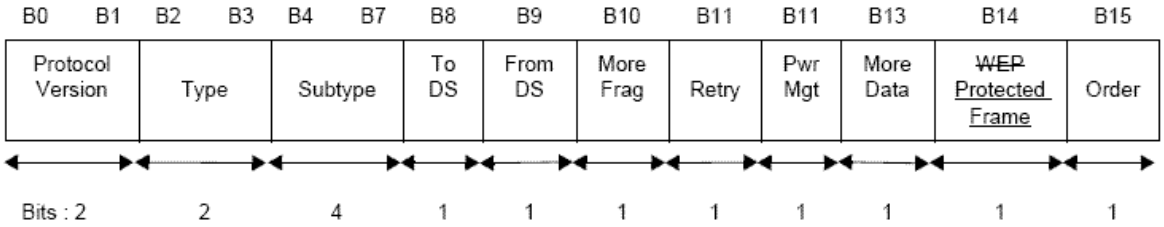
- En MAC header (rammehode) utgjøres av felter for Frame Control, Duration, adressering og sekvenskontroll.
- En variabel frame body som inneholder informasjon avhengig av rammetype (Control, Data eller Management).
- En FCS (Frame Check Sequence) som inneholder en 32-bit lang CRC (Cyclic Redundancy Check)

Figur 2 viser det generelle rammeformatet. Datarammeformatet er likt det generelle rammeformatet. Tallet over hvert rammefelt viser hvor mange oktetter eller byte som er satt av til det respektive feltet.



Figur 2: Det generelle rammeformatet i 802.11 trådløse nett[2]

Frame Control feltet er igjen oppdelt i en rekke felt. Figur 3 viser Fram Control feltets oppdeling, der tallet under hvert felt angir hvor mange bit som er satt av til feltet.



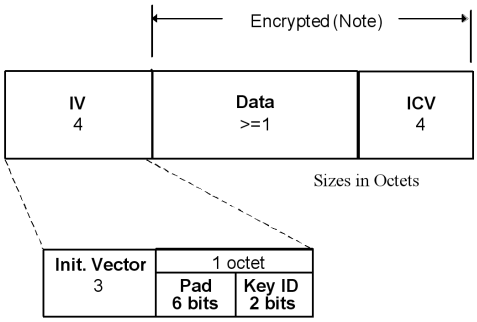
Figur 3: Frame Control feltets oppdeling i det generelle rammeformatet i 802.11[3]

Protocol Version angir versjonsnummer. Verdien er 0. Type feltet angir om rammen er en Control-, Data- eller Managementramme. En dataramme har verdien 10 (desimalverdien 2). Subtype angir hva slags undertype. En dataramme kan ha åtte forskjellige verdier. Eksempelvis vil 0000 representere en dataramme kun inneholdende data.

Det eneste feltet som er spesifisert på nytt eller endret i 802.11i er feltet som het WEP i 802.11. I 802.11i heter det Protected Frame. Det er en bit langt og angir om informasjonen i Frame Body benytter en sikkerhetsmekanisme, i så fall settes det til 1. Biten settes kun til 1 i en dataramme eller en Managementramme av undertype Authentication. I sistnevnte tilfelle er det kun WEP-kryptering som er gyldig.

Når informasjonen i en Frame Body er kryptert utvides den for å inneholde beskrivelse av og nødvendig informasjon om krypteringen. En Frame Body kan ikke være lenger en 2.312 oktetter eller byte, så maksimal informasjon fra overliggende lag, som for eksempel IP-trafikk, er 2.312 byte.

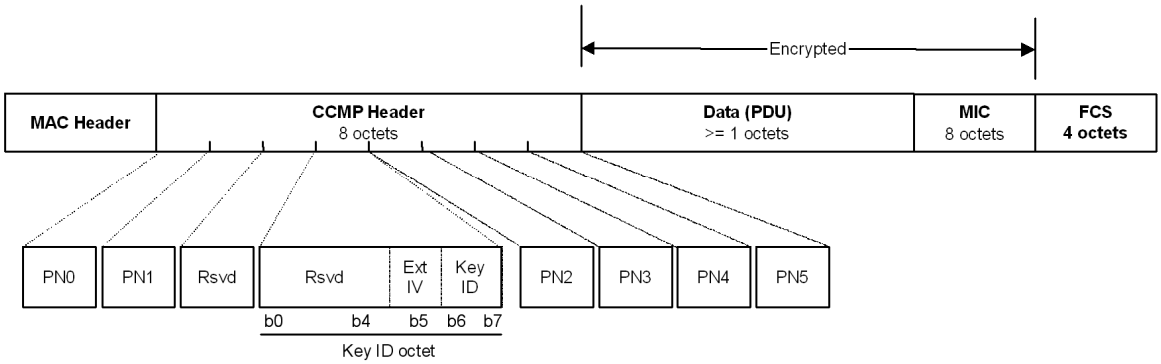
Ved bruk av kryptering benyttes deler av dataplassen for kryptering. Rammeformatet utvides da for å gjøre plass til nødvendig informasjon overført sammen med den krypterte informasjonen. Figur 4 viser hvordan rammeformatet i Figur 2 utvides ved WEP-kryptering. Figur 4 utgjør da Frame Body i Figur 2.



Figur 4: Datarammeutvidelsen ved bruk av WEP-kryptering[2]

Det settes av fire byte til en Initial Vector (IV) først i det som opprinnelig var datafeltet. IV en etterfølges av en kryptert del. Den krypterte delen inneholder den fra overliggende lag overførte informasjonen samt en fire byte lang ICV.

Når CCMP tas i bruk for kryptering, benyttes en annen utvidelse av datarammeformatet. Figur 5 viser hvordan en dataramme blir ved bruk av CCMP.



Figur 5: Datarammeutvidelsen ved bruk av CCMP[3]

CCMP benytter et rammehode på 8 byte (CCMP Header). Der WEP benytter en initialiseringsvektor (IV) på 24 bit benytter CCMP en Packet Number (PN) på 48 bit. Feltet ExtIV benyttes til å signalisere at CCMP hodet er lenger enn og går utover de fire byte som WEP beslaglegger. Feltet/biten settes alltid til 1. Feltet Key ID (to bit) angir nøkkel-ID. De reservertene bitene settes til 0 og ignoreres av partene. MIC er 8 byte lang, og benyttes i stedet for WEPs ICV.

Dersom vi sammenligner datarammeformatet benyttet i WEP og CCMP ser vi at det er satt av dobbelt så mange byte til IV/CCMP-hode og ICV/MIC i CCMP som i WEP. Når maksimal plass satt av til datatrafikk er 2.312 byte, og CCMP kryptering bruker dobbelt så mye plass til å overføre informasjon som ikke er en del av selve dataene fra overliggende lag, f.eks. IP-trafikk, gir dette mindre plass til nyttedata. Dette bør generelt bety at IP-trafikk bruker lenger tid på og overføres i et nettverk som er kryptert med CCMP enn WEP.

Prosentvis økning av Frame Body for å benytte CCMP i forhold til størrelsen når den ikke hadde vært økt (ikke mulig med kryptering) og i forhold til om man benytter WEP for

kryptering er satt opp i Tabell 4. Den opprinnelige Frame Body, informasjon fra overliggende lag (for eksempel IP-pakke) er angitt til 100, 500, 1000 og 1500 byte, og den korresponderende prosentverdi står under.

Tabell 4: Prosentvis økning av Frame Body ved innføring av CCMP

	Pakkestørrelse			
	100 byte	500 byte	1000 byte	1500 byte
Prosentvis økning i forhold til uten kryptering	16,0 %	3,2 %	1,6 %	1,1 %
Prosentvis økning i forhold til WEP-kryptering	7,4 %	1,6 %	0,8 %	0,5 %

For veldig små pakker blir økningen veldig stor. Dette fører til stor økning i overhead for for eksempel VoIP-pakker (Tale over IP). For pakkestørrelser opp mot maksimalverdien (2.312) blir økningen liten. Kommunikasjon der for eksempel IP-pakkene er store bør ikke ha mye påvirkning av dette.

For å se hvordan dette slår ut i praksis i et gitt scenario er det gjennomført tester og målinger for store pakker gjengitt senere i oppgaven. Målingene vil forsøke å avdekke om det er noen målbar forskjell i et praktisk testnett.

3.4 Andre mekanismer

Dette underkapitlet vil ta for seg noen andre mekanismer relevante for innføring av forbedret sikkerhet i trådløse nett ved hjelp av 802.11i. 802.1X, EAP og RADIUS vil forklares i egne kapitler. Disse benyttes i forbindelse med autentisering og nøkkelhåndtering.

3.4.1 802.1X

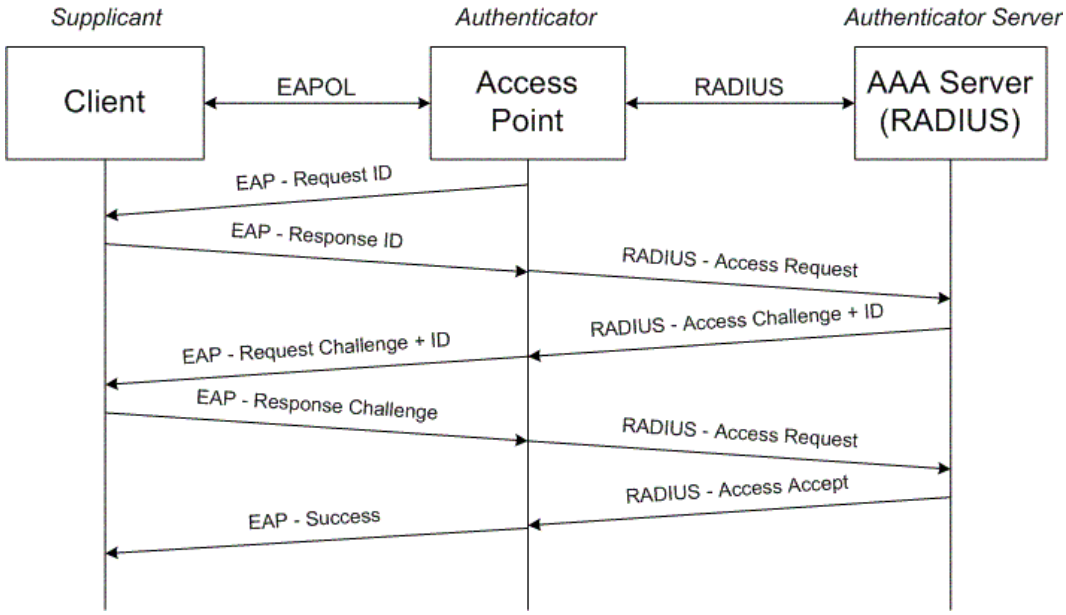
Til autentisering i 802.11i benyttes IEEE 802.1X protokollen. Om det ikke er ønskelig å bruke 802.1X i 802.11i kan det i stedet brukes forhåndsdelt nøkkel (PSK). 802.1X er et rammeverk for autentisering og autorisering av enheter knyttet til nettet. Den forbyr tilgang til nettet inntil autentiseringen er godkjent. 802.1X ble utgitt i 2001 og benytter seg igjen av andre standarder. De viktigste er EAP (Extensible Authentication Protocol)[17] og RADIUS (Remote Authentication Dial-In Service)[18]. EAP er en utvidbar protokoll som gjerne benytter andre standarder igjen. På denne måten kan man benytte egne toppnivå autentiseringsprotokoller til å kjøre oppå EAP. EAP og Radius omtales i egne kapitler.

I de fleste tilfellene er det tre roller involvert i en 802.1X-situasjon:

- Supplicant – Klienten eller brukeren
- Authenticator – Bindeleddet mellom klienten og autentiseringstjeneren
- Autentiseringstjener – Avgjør om supplicanten har avgitt korrekt autentiseringsinformasjon

Figur 6: Roller i en 802.1X-situasjon

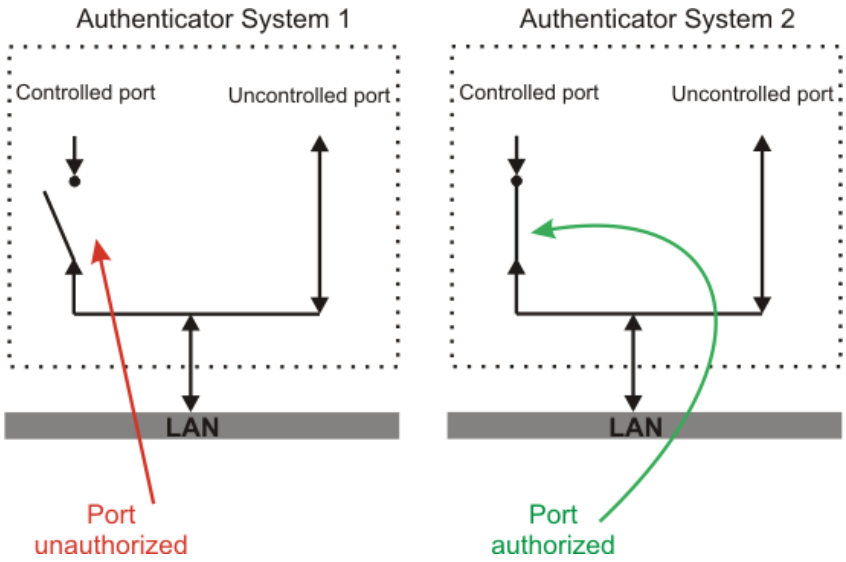
Figur 6 viser de tre enhetene. Supplicant er enheten (representert ved porten den er tilkoblet) som ønsker å få tilgang til tjenestene som tilbys av nettet. I dette tilfelle vil det være den bærbare maskinen. Det trådløse knutepunktet er authenticator, eller en slags dørvakt som krever autentisering før adgang til tjenester i nettet blir tilgjengelig. Autentiseringstjeneren sjekker autentiseringsinformasjonen fra supplicant på vegne av authenticator. Authenticatorens hovedoppgave er å videresende meldinger mellom supplicanten og autentiseringstjeneren. Før supplicanten er autentisert kan den bare kommunisere med authenticatoren som videresender informasjonen til og fra autentiseringstjeneren.



Figur 7: Kommunikasjon for å autentisere klienten[20]

Figur 7 beskriver gangen i autentiseringsmeldingene som blir sendt når en ny klient kommer inn i et trådløst nett. Når klienten mottar EAP-Success meldingen er klienten autentisert, og nøkkelutveksling påbegynnes ved hjelp av 802.11is 4-Way Handshake.

I et nett som benytter seg av 802.1X går autentiseringstrafikken over en ”uncontrolled port”. Anen trafikk i nettet går over en ”controlled port”, og denne er i utgangspunktet lukket. Den åpnes først når klienten er autentisert.



Figur 8: Illustrasjon av Controlled port og Uncontrolled port[19]

I mange sammenhenger er det slik at hvis det hadde vært enkelt, så kunne alle gjort det. 802.1X er relativt komplisert; den inneholder mange nye begreper, og som ellers i sikkerhetsverdenen må alt gjøres riktig hvis det skal ha den tilsiktede effekt. Den er omfattende og lite egnet til bruk i for eksempel et hjem eller andre små nettverk.

3.4.2 EAP

Extensible Authentication Protocol (EAP)[17] er et rammeverk og en protokoll for autentisering som støtter flere forskjellige autentiseringsmekanismer. EAP benyttes av 802.1X og 802.11i. Figur 7 viser hvordan autentiseringsprossesen ved hjelp av EAP foregår.

Når en trådløs node (supplicant) har opprettet kontakt med knutepunktet (authenticator), sender dette en anmodning til noden om å identifisere seg. Noden identifiserer seg, og knutepunktet videresender dette svaret til autentiseringstjeneren. Autentiseringstjeneren sender tilbake en utfordring, som knutepunktet sender videre til noden. Noden beregner svaret basert på den hemmelige nøkkelen, og sender til knutepunktet, som videresender til autentiseringstjeneren. Autentiseringstjeneren gjør samme beregning på utfordringen som noden gjorde, og sammenligner resultatet med det mottatte svaret. Hvis de er like, sender den en EAP-Success til knutepunktet, som først åpner opp for generell kommunikasjon fra noden, og deretter videresender suksessmeldingen til noden, som deretter kan kommunisere fritt.

EAP benytter seg av andre autentiseringsmekanismer, og spesifiserer ikke kryptering. For å beskytte autentiseringsinformasjonen kan man bruke mange forskjellige protokoller på toppen av EAP, for eksempel EAP-TLS, EAP-MD5, LEAP og PEAP.

EAP-TLS[23] representerer en standard sertifikatløsning, og ble introdusert av Microsoft i 1999. EAP-MD5[22] er utviklet av RSA Security og bruker en 128-bit generert streng eller hash. LEAP er en lukket standard utviklet av Cisco Systems. Den har kjente svakheter[24]. PEAP[21] kan benytte sertifikater eller brukernavn/passord, og er utviklet av Microsoft og Cisco.

Tabell 5 gir en oversikt over de nevnte EAP-varianter og en kort sammenligning.

Tabell 5: Sammenligning av utbredte EAP-protokoller[21]

	LEAP (EAP-Cisco)	EAP-TLS	EAP-MD5	PEAP
Produsentstøtte	Utviklet av Cisco. Støttes av begrenset mengde utstyr.	Utbredt støtte.	Utbredt støtte. Anbefales ikke for trådløse nett.	Utbredt støtte fra mange leverandører.
Gjensidig autentisering	Ja, med passord. Svak tjener-autentisering	Ja, med sertifikater	Nei, kun klient-autentisering	Ja, tjenerautentisering med sertifikat, brukerautentisering med brukernavn/passord eller sertifikat
Dynamiske nøkler	Genereres ved autentisering. Dårlig nøkkel-styrke.	Genereres ved autentisering. God nøkkel-styrke.	Nei, statiske.	Genereres ved autentisering. God nøkkel-styrke.
Sikkerhetsnivå	Dårlig ved ordbokangrep.	Sterk.	Ikke sikker.	Sterkeste passordbaserte løsning tilgj.
Basert på standarder	Nei	Ja	Ja	Ja
Beskyttelse av brukercreden-tialer	Kan utsettes for ordbokangrep	Sertifikatbasert autentisering	Kan utsettes for ordbokangrep	Beskyttes av TLS
Klient-autentisering	Nei	Ja, med maskin-sertifikat	Nei	Støtter EAP-metoder som EAP-MSCHAP v2

Dersom EAP-TLS tas i bruk er det nødvendig med utrulling av klientsertifikater, som innebærer administrasjon av et PKI. Krypteringen av brukerdata etter autentisering stopper i basestasjonen for alle mekanismene. Det gir ingen beskyttelse utover den trådløse forbindelsen og må ikke forveksles med en HTTPS/SSL-forbindelse til en webserver. Andre mekanismer må sørge for ende-til-ende-kryptering utover kommunikasjon med knutepunktet.

EAP-metoden som benyttes i testnettet forsøkene og målingene senere i denne oppgaven er utført i er PEAP. Windows XP har innebygget støtte, noe som gjør det enkelt å ta i bruk. Brukere som benytter Windows XP som operativsystem trenger ikke installere tredjepartsløsninger for å autentisere seg. PEAP vil bli benyttet med brukernavn og passord for å identifisere brukeren.

3.4.3 RADIUS

Remote Authentication Dial-In User Service (RADIUS)[18] ble opprinnelig utviklet for å autentisere brukernavn og passord til kunder med oppringte forbindelser til sin internettleverandør. RADIUS er en ”Authentication, Authorization and Accounting” (AAA) protokoll. 802.11i og 802.1X spesifiserer ikke hva slags autentiseringstjener som skal benyttes. RADIUS er en av få muligheter, og svært utbredt. En RADIUS-tjener mottar forespørsler om autentisering av en bruker fra authenticator, autentiserer brukeren og sender tilbake til authenticator den informasjon som er nødvendig for at brukeren skal få de tjenestene han etterspør - tilgang til nettet. Funksjonene i en RADIUS-tjener kan variere, men de fleste kan slå opp brukere i tekstfiler, LDAP-tjenere forskjellige databaser osv.

Forbindelsen mellom authenticator og RADIUS-tjeneren (autentiseringstjeneren) er autentisert gjennom bruk av delte hemmeligheter (shared secrets) som aldri sendes over nettet. Det er foreløpig ingen mekanismer for sikring av basestasjoner utover RADIUS ”shared secret” og administrering av slike involverer litt mange innslag av manuelle rutiner.

Det finnes en rekke implementasjoner av RADIUS, for eksempel FreeRADIUS, en tjener basert på åpen kildekode, og Internet Authentication Service (IAS)[25], som er Microsofts RADIUS tjener og kommer med Microsoft Windows Server. IAS kan benytte seg av Active Directory for å slå opp brukere. Figur 7 viser uteksling av RADIUS-meldinger for autentisering.

3.5 Sammendrag

Innledningsvis ble temaet nettverkssikkerhet introdusert og IEEE 802.11, standarden for trådløse nett, omtalt. Sikkerhetsmekanismen WEP og dens svakheter ble forklart. Videre har forbedringene i tillegget 802.11i blitt gjort rede for samt de mekanismer standarden tar i bruk. Sikkerhetsmekanismen CCMP benyttes i stedet for WEP, og gir kryptering, integritetsbeskyttelse og gjenspillingsbeskyttelse. 802.1X står for autentisering og nøkkelhåndtering. I neste kapittel gis et eksempel på et nettverk med trådløse knutepunkter og hvordan det kan oppgraderes til 802.11i. Oppsett av et testnett beskrives også.

4 Oppgradering til 802.11i og oppsett av testnett

Dette kapitlet benytter som et eksempel på et nettverk med trådløse knutepunkter som kan oppgraderes til 802.11i nettverket til Universitetsstudiene på Kjeller (UniK). Oppsett av et testnett som kan anvendes til senere forsøk og tester for å se om det i praksis kan måles noen forskjell på performance beskrives.

4.1 Oppgradering til 802.11i

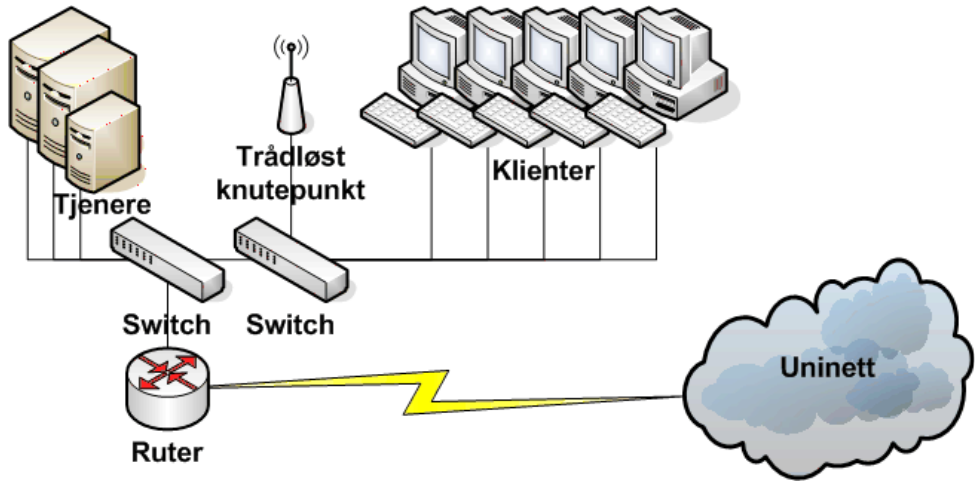
Nettverket til Universitetsstudiene på Kjeller (UniK) vil benyttes som eksempel på oppgradering av sikkerhet i 802.11 trådløse nettverk.

4.1.1 Beskrivelse av UniKs nettverk

UniKs nettverk består bl.a. av:

- ca 120 stasjonære arbeidsstasjoner
- 19 servere
- 12 skrivere
- trådløse knutepunkt

De forskjellige enhetene er koblet sammen til et nettverk ved hjelp av standard Ethernet-switcher og tilknyttet omverden ved hjelp av en ruter (kjeller-gw.uninett.no) med forbindelse til UniNett (oslo-gw1.uninett.no) (Unntatt kjellerinstituttene som er tilknyttet kjeller-gw.uninett.no).



Figur 9: Prinsippskisse av UniKs nettverk

Unik er tildelt IP-nettene 193.156.96 og 97. Ruteren som forbinder UniKs nettverk med omverdenen har IP-adresse 193.156.96.1. Tjenerne frigg.unik.no (193.156.96.17) er DHCP-tjener. Tjeneren moskva.unik.no (193.156.97.30) er RADIUS-tjener. Unik har følgende trådløse nett:

1) Innendørsnett (UNIK_Wlan)
2) Utendørsnett (Unik)
3) Hybelhusnett (hybelhuset)

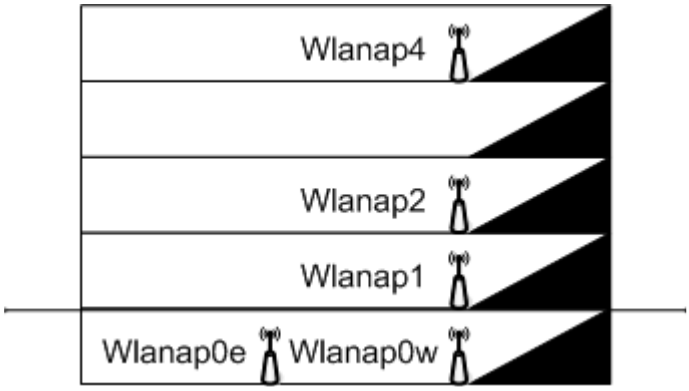
Hybelhusnettet er et åpent, ukryptert nett utenfor brannmuren, og sørger for internett forbindelse i Hybelhuset mellom FFI og Unik. Utendørsnettet er også et åpent ukryptert nett som dekker utearealene utenfor UniK, slik at man kan være tilknyttet Internett når en benytter utearealene.

Innendørsnettet (UNIK_Wlan) blir gjenstand for videre interesse. Det består av en del knutepunkter som besørger forbindelse til UniKs interne nett samt Internett. Det er først og fremst et tilbud til studentene, slik at de med enkelthet skal kunne koble sine bærbare maskiner til Internett. Nettet er kryptert med WEP-40. Nøkkelen er publisert på UniKs hjemmeside. Ansatte, stipendiater og studenters brukernavn og passord utdeles av Drift. Brukernavn og passord brukes bl.a. for å få tilgang til e-post samt å logge på Windows-domene. Tabell 6 viser en oversikt over knutepunktene i innendørsnettet.

Tabell 6: Knutepunktene i UniKs interne nett

Navn	IP-adresse	Modell	Firmware	Lokasjon
Wlanap0w.unik.no	193.156.97.9	Orinoco AP-700	v2.6.0	U.etg.
Wlanap0e.unik.no	193.156.97.10	Orinoco AP-700	v2.6.0	U.etg.
Wlanap1.unik.no	193.156.97.11	Orinoco AP-600	v2.4.5	1.etg.
Wlanap2.unik.no	193.156.97.12	D-Link DWL-2100AP	v2.00eu	2.etg.
Wlanap4.unik.no	193.156.97.13	D-Link DWL-2100AP	v2.00eu	4.etg.

Figur 10 illustrerer lokasjonen til knutepunktene i Tabell 6.



Figur 10: Visualisering av knutepunktplassering

Disse knutepunktene har vært anskaffet over tid, og er derfor en broket masse. Den siste anskaffelsen var Orinoco AP-700 knutepunktene som erstattet et D-Link DWL-2100AP, grunnet behov for utvidet kapasitet i Auditoriet. AP-700 har mulighet til å fordele lasten mellom seg automatisk for å oppnå optimal ytelse. Auditoriet rommer normalt plass til 60 personer. Når det arrangeres kurs og seminarer med så mange samtidige brukere, går det tregt når alle skal utføre de samme operasjonene på en gang. Knutepunktene av merke D-Link

DWL-2100AP støtter ikke 802.11i. Siden AES-kryptering krever betydelig mer ressurser enn WEP-kryptering er det lite sannsynlig at de kan støtte 802.11i ved hjelp av en oppgradering av firmware.

Knutepunktene med modellbetegnelse AP-700 støtter 802.11i med den firmware-versjonen de kjører. Orinoco AP-600 støtter 802.11i fra og med firmware-versjon 2.5.2 av oktober 2004. Wlanap1.unik.no/193.156.97.11 kjører pr. 22. august 2005 versjon 2.4.5.

4.1.2 Behov for sikkerhet

Ved å konvertere til 802.11i og CCMP kan UniK bedre og modernisere den trådløse sikkerheten. WEP er mangelfull og det tar kort tid å finne nøkkelen. Ved å finne nøkkelen kan en inntrenger bl.a. få tilgang til nettet, lese og lagre kommunikasjon, spille av kommunikasjon på nytt i opprinnelig eller endret, utnytte de ressursene som er tilgjenglig i nettet til for eksempel ulovlige formål.

Mer konkrete eksempler på slikt kan være:

- Bruk av UniKs internettforbindelse til lovlig eller ulovlig bruk som nedlasting av store filer, piratkopiert video eller musikk eller barnepornografi eller andre straffbare handlinger. Siden UniK har 1 Gbit/sek forbindelse til Internett vil nok ikke en inntrenging på et trådløst nett med teoretisk datarate på 54Mbit/sek utgjøre en voldsom trussel. Utnyttelse til ulovlige formål er en annen sak.
- Når en bruker har tilgang til innendørsnettet til UniK er brukeren på innsiden av brannmuren. Angrep som ville vært filtrert bort kan fungere for angriperen når han er på innsiden. Ved å sette maskinen rieekan.unik.no (193.156.96.31), som fungerer som ssh.unik.no, ut av spill og overta IP-adressen kan en angriper logge innloggingsforsøk og avlese brukernavn og passord dersom en innlogget bruker ikke har logget inn før, eller ignorerer advarselen om at maskinen ikke er den samme eller har fått ny vertsnøkkel.
- Når en bruker eller inntrenger har tilgang til et WEP-kryptert trådløst nett ser ikke bare maskinen sin egen trafikk, men også trafikken til alle de andre maskinene i det trådløse nettet. Det går mye usikret trafikk i et nettverk, som for eksempel e-post. POP er en svært utbredt protokoll for å hente e-post. Denne sender all informasjon i klartekst, inkludert brukernavn og passord. Som mange andre steder har brukerne på UniK samme passord på e-post som Linux, Windows og andre tjenester som krever innlogging. Har en først tilgang til e-postpassordet har en ofte tilgang til brukerens andre tjenester

CCMP kan også benyttes med forhåndsdelt nøkkel, men ved å benytte 802.1X for autentisering og nøkkelhåndtering kan behovet for å huske nettverkspassord elimineres. I stedet kan brukernavn med tilhørende passord benyttes. 802.1X kan benyttes sammen med eksisterende autentiseringstjener for å få tilgang til UniKs brukerdatabase.

Ved å ta i bruk 802.1X er det heller ikke lenger nødvendig å bytte nettverksnøkkel når den har kommet på avveie eller noen som har fått tilgang til den ikke lenger skal ha det. Individuelle brukere kan nektes tilgang til det trådløse nettet gjennom endring av rettigheter i brukerdatabasen. En bruker, som for eksempel en gjest kan gis tilgang i spesielle eller begrensede tidsrom.

Oppsett av 802.11i nettverk er beskrevet i eget underkapittel der nettverket med alle komponentene settes opp fra grunnen av.

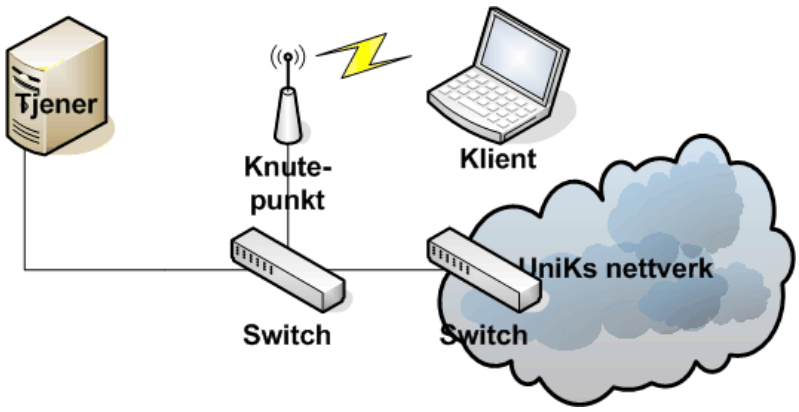
4.2 Oppsett av testnett

Oppsett og konfigurasjon av et testnett er beskrevet i dette underkapitlet. En detaljert steg-for-steg oversikt finnes i appendiks. Informasjonen er også relevant der det allerede eksisterer et trådløst nettverk der sikkerhetsmekanismene skal oppgraders. Valgene er tatt på grunnlag av at det skulle vært en passende konfigurasjon for UniKs trådløse nett. Til de senere forsøk og tester benyttes testnettet.

4.2.1 Konfigurasjon

Ved oppsett av eller oppgradering til 802.11i med 802.1X-autentisering er det foruten et eller flere knutepunkt behov for en RADIUS-tjener[18]. Oppgaven til en RADIUS-tjener er å ta i mot og behandle autentiseringsforespørsler. Det eksisterer flere produsenter av RADIUS-tjenere, og Microsofts Internet Authentication Service (IAS) er nevnt tidligere. IAS er et tillegg i Microsoft Windows Server.

Testnettet ble satt opp med Microsoft Windows Server 2003 Enterprise Edition med Internet Authentication Service som RADIUS-tjener. Som trådløst knutepunkt ble et nytt Orinoco AP-700 valgt. Disse to enhetene ble koblet sammen med en Focus Networks 10/100 Switch. Deretter ble switchen tilknyttet UniKs nett. En Fujitsu-Siemens Amilo Pro V2020 med trådløst nettverkskort ble benyttet som trådløs klient.



Figur 11: Skisse av testnettet

Knutepunktet som benyttes i testnettet, Orinoco AP-700 er det samme som nyanskaffelsene til UniK. Det ble konfigurert ved hjelp av en nettleser. Ved å taste inn knutepunktets IP-adresse i en nettleser gis adgang til et konfigurasjonsgrensesnitt. Ved første gangs navigasjon til knutepunktets nettside åpnes en veiledning. Veiledningen gir steg-for-steg muligheten til å legge inn bl.a. systemkonfigurasjon, velge IP-konfigurasjon, angi passord, velge driftsmodus og nettverksnavn. Etter at veiledningen fullfører oppsummeres valgene som er utført. De andre innstillingene som ikke er med i oppstartsveiledningen må endres etterpå. Tabell 7 viser de viktigste innstillingene som knutepunktet ble satt opp med.

Tabell 7: Et utvalg av knutepunktets innstillinger

Innstilling	Verdi
IP-adressetildeling	Dynamisk
IP-adresse	193.156.97.232
Subnettmaske	255.255.254.0
Gateway IP-adresse	193.156.96.1
Nettverksnavn (SSID)	UNIK_Test
Kanal	11
Sikkerhetsmodus	802.11i
RADIUS-tjener	193.156.97.238
Autentiseringsport	1812

Den trådløse klienten som benyttes i dette testnettet er en Fujitsu-Siemens Amilo Pro V2020 med Windows XP Professional. Det trådløse kortet er et Intel PRO/Wireless 2200BG med firmware 0.1.4. Driveren ble oppgradert til 9.0.2.31 av 19.7.2005 for å støtte WPA2. For at Windows XP skal støtte 802.11i/WPA2 installeres en oppdatering[28] til operativsystemet. Det ble oppdaget at den opprinnelige driveren ikke støttet WPA2 etter å ha installert oppdateringen fra Microsoft. Det kan gjøres ved å kontrollere om valget WPA2 kommer opp i listen ”Nettverksgodkjenning” under konfigurasjon av et trådløst nettverk i Windows XP. Mangler valget støtter ikke driveren 802.11i. IEEE 802.1X-godkjenning aktiveres for nettverket og EAP-type settes til Beskyttet EAP (PEAP).

Ved å velge PEAP som EAP-type i dette nettverket velges en løsning som ikke nødvendiggjør en egen PKI-infrastruktur. Kun tjeneren installerer et sertifikat for å identifisere seg selv, mens brukerne identifiserer seg med brukernavn og passord. PEAP er den sterkeste passordbaserte løsningen tilgjenglig[21]. Brukernavnet og passord beskyttes av TLS når det sendes mellom brukeren og autentiseringstjeneren. Andre brukernavn og passordbaserte løsninger som for eksempel LEAP kan være utsatt for ordbokangrep. Det er innebygget støtte for PEAP i Windows XP, og den utbredte XSupplicant for Linux støtter også PEAP. En annen gevinst ved å velge PEAP er at brukeren ikke trenger å installere andre supplicanter for å benytte 802.1X aktivert nettverk når han alt bruker Windows XP eller XSupplicant.

På den trådløse klienten settes innstillingen til at tjenersertfikatet ikke skal bekreftes av en klarert rotsertifiseringsinstans. I testnettet installeres et sertifikat på autentiseringstjenerne generert av egen maskin. I en installasjon i UniKs nettverk vil dette kanskje ikke være et naturlig valg. I et nett der man for eksempel tilbyr tilgang til allmennheten vil det være naturlig å installere et sertifikat signert av utsteder i en kjede der rotsertifiseringsinstansen er klarert på forhånd.

Til slutt velges at klienten ikke skal benytte seg automatisk av Windows-påloggingsnavnet og passordet for å gi brukeren anledning til å taste inn dette selv. I testnettet er det likegyldig hva som velges, siden vilkårlige brukernavn og passord kan settes. På maskiner som benyttes i UniKs trådløse nettverk, men ikke er en del av Windows-domene, vil det kanskje også være naturlig å velge at brukernavn og passord tastes inn manuelt da sannsynligheten for at det systemadministratortildelte brukernavn og passord ikke er det samme som benyttes lokalt på maskinen.

4.2.2 Oppsetting

RADIUS-tjeneren, Internet Authentication Service, ble installert på en Microsoft Windows 2003 Server Enterprise Edition. Installasjonen ble utført ved at en evaluation edition av Microsoft Windows 2003 Server ble lastet ned fra Microsofts hjemmeside, brent til CD og startet opp fra på maskinen som skulle benyttes. En enkel og standard konfigurasjon ble valgt som utgangspunkt ved å følge installasjonsveiviseren.

Etter installasjonen av operativsystemet oppdateres systemet med de siste sikkerhetsoppdateringer fra Microsoft. "Certificate Services" installeres fra kontrollpanelet. Denne modulen gjør tjeneren i stand til å utstede sertifikater. Senere ble et sertifikat utstedt til tjeneren ved hjelp av nettleseren. Sertifikatet autentiserer tjeneren ovenfor klienten.

Internet Authentication Service ble også installert fra kontrollpanelets "Add/Remove Programs" og "Networking Services". Ved hjelp av Active Directory Installation Wizard gjennomgås en veiviser for å konfigurere tjeneren som domenekontroller. En gruppe opprettes for å gi medlemmene Remote Access rettigheter. Tre brukere legges inn for testing, og medlemskap i gruppen opprettes. IAS konfigureres til å logge autentiseringsinformasjon til en lokal fil. Filformatet forklares i [31]. Denne ressursen er svært verdifull under feilsøking og lesing av loggfilen.

Hvert trådløst knutepunkt som skal kommunisere med en RADIUS-tjener må registreres i autentiseringstjeneren som RADIUS-client. I IAS registreres IP-adresse og delt hemmelighet for hvert knutepunkt. I testnettet ble en kort streng som er lett å huske benyttet. En streng på mer enn 22 tegn, med en god blanding av karakterer bør benyttes[32]. I tillegg sjekkes konfigurasjonen for å være viss om at standard port for autentisering 1812 benyttes. En ny Remote Access Policy settes opp for at gruppen med brukere som skal kunne benytte det trådløse nettet, og benytte PEAP.

En mer detaljert beskrivelse av fremgangsmåten for installasjonene beskrevet ovenfor finnes i appendiks.

4.3 Sammendrag

Dette kapitlet har beskrevet et eksempelnettverk som kan oppgraderes til 802.11i, og belyst noen momenter som taler for det. Oppgradering av sikkerheten til 802.11i/WPA2 og CCMP på dette tidspunkt kan føre til at mange brukere må oppdatere eller bytte ut maskinvare eller programvare fordi brukernes utstyr i utgangspunktet er ikke er klart til å ta i bruk den nye standarden. For eksempel kan det hende at halvparten av brukerne må bytte ut den trådløse modulen i sine bærbare maskiner for å kunne oppgradere. Dette vil merkes i organisasjonen. Videre beskrives oppsett av testnettet som benyttes i forsøkene i neste kapittel. I neste kapittel skal performance måles for å forsøke og avdekke forskjeller i performance i trådløse nettverk som benytter CCMP i forhold til WEP.

5 Forsøk

I dette kapittelet gjennomføres prøver og forsøk for å se om throughput (gjennomstrømningshastigheten) på nettverkslaget påvirkes ved å oppgradere til 802.11i og benytte CCMP som sikkerhetsmekanisme i stedet for WEP. Prøvene og forsøkene har vært utført i testnettet.

Tidligere har sikkerhetsmekanismenes utvidelse av rammestrukturen blitt gjort rede for. Forsøkene har til hensikt å forsøke å måle denne endringen i testnettet. Programmet Iperf vil benyttes for å måle throughput.

5.1 Programvare

I forbindelse med forsøkene har følgende programmer blitt benyttet:

- Iperf: Iperf er et verktøy for å måle et nettverks performance. Iperf ble utviklet som et moderne alternativ til andre programmer som begynner å bli gamle og kan være vanskelige å bruke. Iperf kan måle TCP og UDP performance og være nyttig i tuning av forskjellige parametere. Det kan gi tilbakemelding om throughput, forsinkelse, jitter og tap av datagram. I forsøkene har Iperf blitt benyttet til å måle throughput.
- Ethereal: Ethereal er en nettverksprotokollanalysator med funksjoner for å analysere og feilsøke protokoller og programvare. Ethereals kildekode er åpen, og programmet distribueres under GNU Public License. I forsøkene har Ethereal blitt benyttet bl.a. til å analysere trafikken i UniKs nettverk.
- Netstumbler: Netstumbler er et Windows-program for å finne 802.11 trådløse nettverk. Programmet rapporterer nettverksnavn, kryptering, signalstyrke, kanal osv. Programmet kan benyttes til å verifisere en installasjon, finne plasser i nettverket med dårlig dekning, undersøke hvilke kanaler som er i bruk på en lokasjon osv. Netstumbler er et gratisprogram. I forsøkene har Netstumbler blitt benyttet for å avdekke eventuelle andre trådløse knutepunkt i nærheten av testnettet.

5.2 Performance – Måling av throughput med Iperf

Denne testen har til hensikt å sette opp en IP-forbindelse mellom klientmaskienen og tjeneren, og måle hvor mye IP-trafikk som kan overføres i løpet av et gitt tidsrom. Først settes forbindelsen opp over en link kryptert med WEP, og etterpå med CCMP. Til slutt vil målingene sammenlignes for å forsøke å avdekke forskjeller. Til å måle throughput anvendes Iperf.

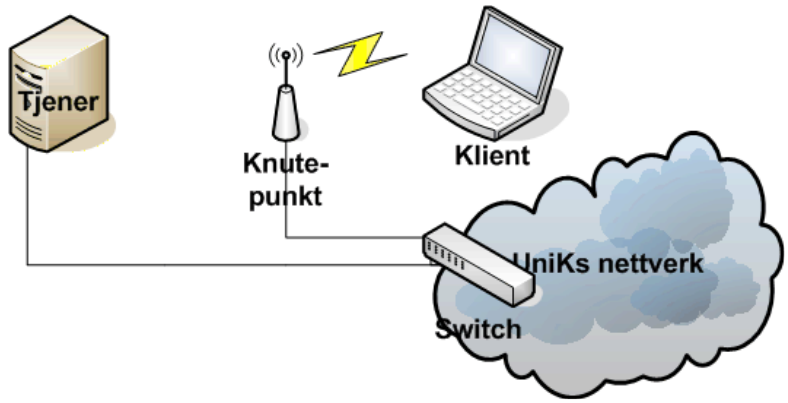
5.2.1 Forundersøkelse

Før selve testen ble det gjennomført en liten forundersøkelse, bestående av tre forsøk på totalt ni målinger, for å undersøke hvilke verdier for throughput som kunne forventes. Maskinene mottar IP-adresser automatisk fra DHCP-tjeneren. Ved hjelp av Netstumbler ble det avdekket at det ikke var noen knutepunkt i nærheten som benyttet samme kanal. Det var heller ingen andre brukere enn testklienten tilknyttet knutepunktet. Forundersøkelsen er gjennomført med CCMP som sikkerhetsmekanisme og 802.1X for autentisering. På tjeneren ble Iperf startet med kommandoen "iperf –s", der –s angir at programmet skal kjøre i tjenermodus. På klienten startes hvert gjennomløp med kommandoen "iperf –c IP-adresse", der –c angir at programmet skal kjøre som klient. IP-adresse er IP-adressen til tjeneren. Figur 12 viser et eksempel på utskrift til skjerm.

```
------------------------------------------------------------
Client connecting to 193.156.97.208, TCP port 5001
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[1856] local 193.156.97.202 port 3367 connected with 193.156.97.208 port 5001
[ ID] Interval       Transfer     Bandwidth
[1856]  0.0-10.0 sec  16.5 MBytes  13.8 Mbits/sec
```

Figur 12: Skjermutskrift fra Iperf

Forundersøkelsens tre første målinger utføres med et modifisert testnett. Knutepunktet og tjeneren er koblet utenom Focus switch. Trafikken mellom knutepunktet og tjeneren vil være utsatt for påvirkninger og forsinkelser fra annen trafikk i UniKs nettverk. Denne konfigurasjonen vil være nærmest en reell konfigurasjon i UniKs nettverk: Et knutepunkt og en server vil være direkte tilknyttet UniKs switch. Hensikten med denne konfigurasjonen er å undersøke hvilke verdier en trådløs bruker kan forvente seg i UniKs trådløse nettverk. Figur 13 viser det modifiserte testnettet benyttet i forundersøkelsens målinger en, to og tre.



Figur 13: Testnettets konfigurasjon under forundersøkelsens måling en, to og tre.

En måling utføres ved å angi kommandoen iperf –c 193.156.97.208. Denne kommandoen kjøres tre ganger etter hverandre. De tre første målingene ga en gjennomsnittshastighet på 5,84 Mbit/sek. Dette er lavt, og langt under hva en kan forvente i et trådløst nett med teoretisk hastighet 54 Mbit/sek. Den teoretiske hastigheten 54 Mbit/sek er på fysisk lag, men viktigst er det en teoretisk hastighet. Maksimal gjennomstrømningshastighet på MAC laget er omtrent 27 Mbit/sek ved datapakker på 1500 byte for et 802.11 nett konfigurert kun for 54 Mbit/sek teoretisk hastighet[29]. Knutepunktet i testnettet er konfigurert for klienter som kan kjøre både 11Mbit/sek og 54Mbit/sek, men klienten opererer kun i 54Mbit/sek-modus og uten andre klienter i nettverket. Dette innebærer at hastigheten praktisk ikke kan oppnå 27Mbit/sek

grunnet en ekstra beskyttelsesmekanisme (CTS-to-self) på lavere lag i OSI-modellen som er aktivert når 54Mbit/sek nettverk settes opp til å støtte 11Mbit/sek klienter[29]. Når det er trådløse noder i nettverket som ikke støtter høyere hastigheter enn 11Mbit/sek, benyttes en høyere Slot Time (tid mellom rammer) som er med på å øke overhead i nettverket. Noen noder som ikke støtter høyere hastigheter enn 11Mbit/sek støtter heller ikke Short Preamble (hodefelt på fysisk lag). Ved bruk av Long Preamble økes overhead ytterligere.

Tabell 8: Forundersøkelsens måling 1, 2 og 3 med konfigurasjon som vist i Figur 13

Forsøk	Tid	Overført	Throughput
1	10,0 sek	5,80 MB	4,85 Mbit/sek
2	10,0 sek	8,13 MB	6,79 Mbit/sek
3	10,0 sek	7,03 MB	5,87 Mbit/sek
Gjennomsnittlig		6,99 MB	5,84 Mbit/sek

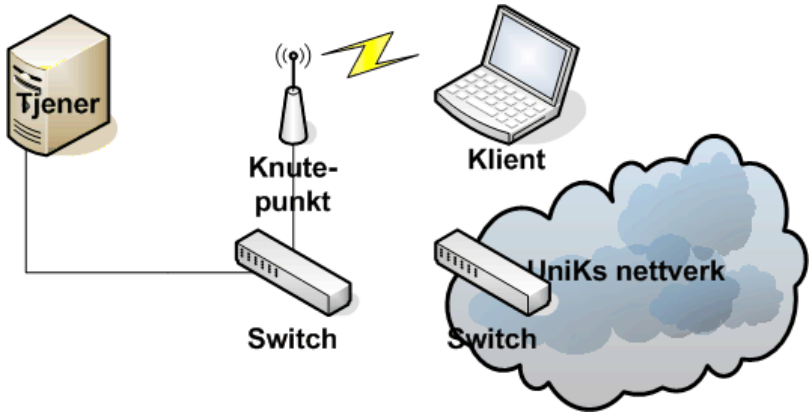
For å redusere påvirkningen fra UniKs nettverk kobles Focus Switch inn igjen før videre målinger. Knutepunktet og tjeneren er koblet til UniKs nett gjennom Focus switch. Testnettet settes tilbake til tidligere konfigurasjon. Figur 11 viser konfigurasjonen benyttet under forundersøkelsens målinger tre, fire og fem. Tre nye målinger ble foretatt. Tabell 9 viser resultatet fra disse målingene. Gjennomsnittsverdien ble 13,6 Mbit/sek.

Tabell 9: Forundersøkelsens måling 4, 5 og 6 med konfigurasjon som vist i Figur 11

Forsøk	Tid	Overført	Throughput
4	10,0 sek	16,3 MB	13,6 Mbit/sek
5	10,0 sek	16,0 MB	13,4 Mbit/sek
6	10,0 sek	16,5 MB	13,8 Mbit/sek
Gjennomsnittlig		16,3 MB	13,6 Mbit/sek

13,6 Mbit/sek er langt bedre enn 5,84 Mbit/sek, men fremdeles lavt.

Testnettet settes så til den konfigurasjon det hadde under hovedtestens forløp. Testnettet frakobles UniKs nettverk. Nettet ser ut som over, men forbindelsen mellom de to switchene er borte. Testnettet har ikke lenger noen kontakt med omverdenen, og burde oppnå høyere hastigheter. Figur 14 viser denne konfigurasjonen. Selv om testnettverket bruker automatisk tilordnede IP-adresser er de allerede tilordnet, og videre forsøk kan gjennomføres med disse.



Figur 14: Testnettets konfigurasjon under forundersøkelsens del tre

Når de siste tre målingene i forundersøkelsen gjennomføres er tjeneren og knutepunktet et isolert testnett. Klienten er den eneste trådløse stasjonen tilknyttet knutepunktet. Trafikken i den trådbundne delen av testnetter er ikke forstyrret av utenforstående enheter. Eventuelle forstyrrelser i det trådløse nettet er ikke endret.

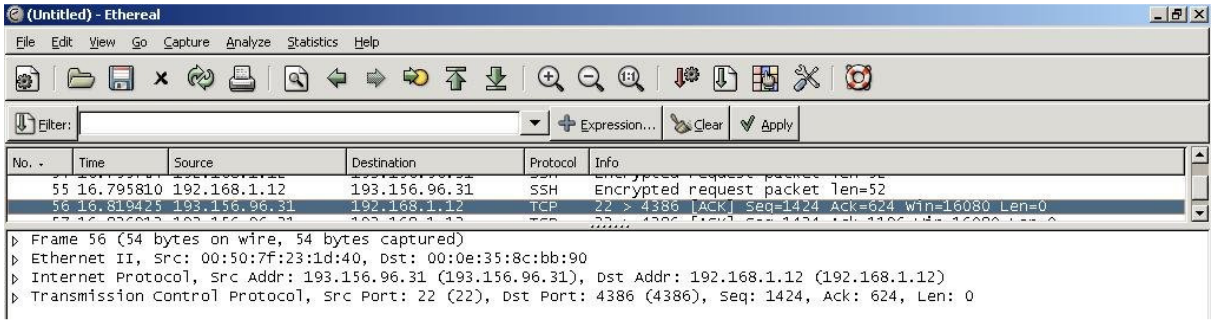
Tre målinger gir en gjennomsnittshastighet på 21,7 Mbit/sek. Tabell 10 viser målingene.

Tabell 10: Forundersøkelsens måling 7, 8 og 9 med konfigurasjon som vist i Figur 14

Forsøk	Tid	Overført	Throughput
7	10,0 sek	25,4 MB	21,3 Mbit/sek
8	10,0 sek	26,3 MB	22,1 Mbit/sek
9	10,0 sek	25,8 MB	21,6 Mbit/sek
Gjennomsnittlig		25,8 MB	21,7 Mbit/sek

Når gjennomsnittlig overføringshastighet av IP-trafikk i siste del av forundersøkelsen har nådd 21,7 Mbit/sek kan det syntes som at et maksimalt potensial for det konfigurerte testenettet er nådd. Konfigurasjonen benyttet under disse tre siste målinger vil brukes i performance-testen.

Ved denne forundersøkelsens målinger en til og med seks var testnettet koblet til UniKs nett. Under måling syv, åtte og ni var testnettet isolert. De første seks målingene gav bemerkelsesverdig lavere verdier enn de tre siste. Dette må skyldes en stor påvirkning. For å forsøke å avdekke hva dette skyldes ble en pakkeanalysator kalt Ethereal installert for å ha muligheten til å titte nærmere hva slags IP-trafikk som overføres i UniKs nett. Ethereal ble innstaller på tjeneren i testnettet. Testnettet ble midlertidig tilkoblet UniKs nett. Pakkeanalysatoren ble så satt til å innhente noen sekunders IP-trafikk.



Figur 15: Eksempel på skjermbilde fra Ethereal

Antall pakker mottatt per sekund ble ca 104. Ved en rask gjennomgang av de innsamlede pakker viser det seg at de aller fleste pakkene kommer fra samme node. Denne spesielle noden sendte veldig mye IP-trafikk, store mengder pakker som ble mottatt av alle maskinene i nettet. En sjekk av denne noden viste at den var en videotelefonikodek som kontinuerlig sendte IP-pakker ut i nettet, og distribuerte video i sanntid. Dette må være årsaken til at hastigheten var bemerkelsesverdig lav så lenge knutepunktet og tjeneren var tilknyttet UniKs nettverk, da dette var det eneste som ble endret gjennom forundersøkelsen.

Forundersøkelsen viste at hastigheten over et trådløst knutepunkt var ca 21-22Mbit/sek. De forskjellige resultatene fra forundersøkelsens tre deler kan ikke skyldes noe annet enn koblingen av nettverket, som vist ved hjelp av figurer, da dette er det eneste som ble endret

mellom hver av forundersøkelsens deler med tilhørende resultater vist i tabellene. Når et stort antall pakker sendes gjennom samme switch som strømmen av data som sendes i forundersøkelsen blir det trangt om plassen. Det syntes som om at den store mengden pakker som ble sendt til alle nodene i UniKs nett krevde mye plass i overføringsmediet slik at dataene som måler throughput fikk mindre plass. På denne måten kom mindre måledata gjennom nettverket og throughput ble målt til de lave tallene som vises i Tabell 8. Når kilden til den store mengden pakker som kom fra UniKs nett ble flyttet et hakk lenger unna ved å sette inn Focus Switch som vist i Figur 11, kom tydeligvis testnettes tjener og knutepunkt nærmere hverandre slik at mer måledata kom gjennom slik resultatet vises i Tabell 9. Når testnettet i siste del av målingene ble isolert fra UniKs nett trengte ikke lenger måledataene kjempe om plassen i overføringsmediet og kunne benytte ressursen fullt ut. Da rapporteres riktig throughput som vist i Tabell 10.

Performance-testen skal forsøke å avdekke om det i praksis er noen forskjell på throughput om CCMP benyttes fremfor WEP til å sikre kommunikasjonen i et trådløst nettverk.

5.2.2 Måling av Performance med WEP og CCMP

Denne testen har til hensikt å avdekke forskjeller i throughput ved bruk av CCMP fremfor WEP i 802.11i nettverk. Til å gjennomføre testene benyttes testnettet. Figur 14 viser konfigurasjonen. For å eliminere feilkilder er følgende momenter tatt i betraktning:

- Det trådløse knutepunktet og tjeneren er de eneste noder knyttet sammen i den trådbundne delen av testnettet for å unngå forstyrrende trafikk.
- Den trådløse klienten er den eneste klienten tilknyttet knutepunktet.
- Knutepunktet arbeider uforstyrret uten andre knutepunkt innen rekkevidde, og valgt kanal er ulik andre kjente knutepunkter i nærheten, utenfor rekkevidde.

Det trådløse knutepunktet, tjeneren og klienten hadde alt mottatt IP-adresser fra tjeneren i UniKs nett som dynamisk tildeler IP-adresser, slik at det ikke var nødvendig å konfigurere IP-adresser selv om enhetene i nettverket ikke hadde tilgang på DHCP-tjener. Alle testene er utført med samme knutepunkt og samme tjener. Noen parametere ble forandret mellom testene med WEP og CCMP som sikkerhetsmekanisme. Tabell 11 gir en oversikt over hvilke parametere i knutepunktet som ble endret, og hvilken verdi de hadde under de forskjellige målingene.

Tabell 11: Parametere ulike under forsøk

Parameter	WEP	CCMP
Security profile	WEP Station	802.11i Station
Autentisering	Åpen	802.1X

Testen med WEP som sikkerhetsmekanisme ble utført først. Kommandoen iperf –c 193.156.97.208 ble kjørt fra klienten ti ganger etter hverandre. Tabell 12 lister verdiene fra målingene. Gjennomsnittet av alle målingene ble 21,7 Mbit/sek.

Tabell 12: Resultatene fra ti båndbreddemålinger med WEP som sikkerhetsmekanisme

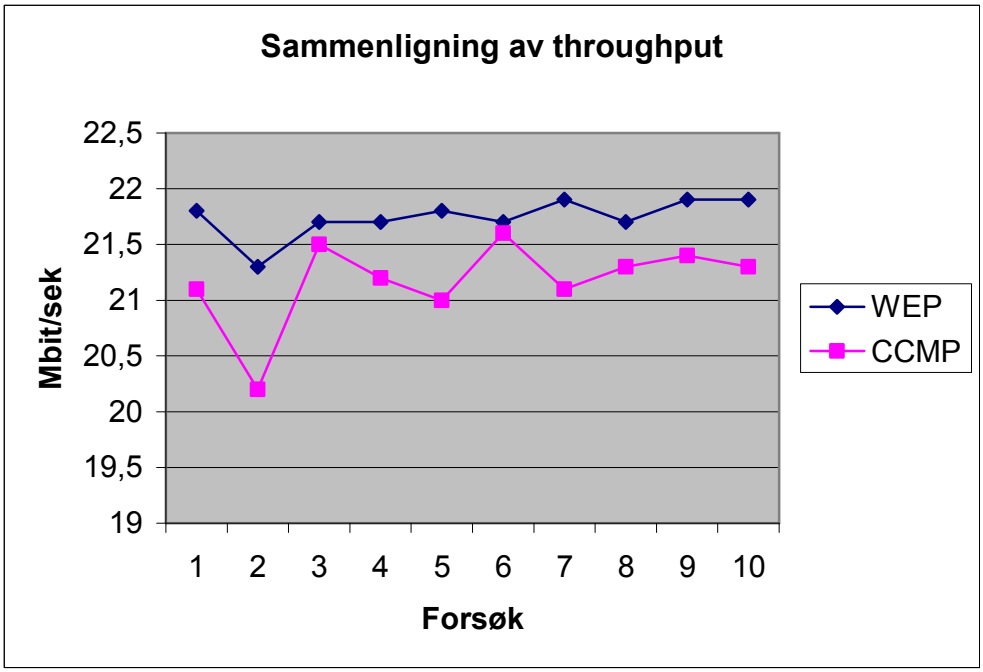
Forsøk	Tid	Overført	Throughput
1	10,0 sek	25,9 Mbyte	21,8 Mbit/sek
2	10,0 sek	25,4 Mbyte	21,3 Mbit/sek
3	10,0 sek	25,9 Mbyte	21,7 Mbit/sek
4	10,0 sek	25,9 Mbyte	21,7 Mbit/sek
5	10,0 sek	26,0 Mbyte	21,8 Mbit/sek
6	10,0 sek	25,9 Mbyte	21,7 Mbit/sek
7	10,0 sek	26,1 Mbyte	21,9 Mbit/sek
8	10,0 sek	25,9 Mbyte	21,7 Mbit/sek
9	10,0 sek	26,1 Mbyte	21,9 Mbit/sek
10	10,0 sek	26,1 Mbyte	21,9 Mbit/sek
Gjennomsnittlig		25,9 Mbyte	21,7 Mbit/sek

Etter at de første ti målingene var blitt utført ble parametrene i knutepunktet som definerer sikkerhetsmekanismene endret. Med samme kommando som i de ti første målingene ble det innhentet data for CCMP som sikkerhetsmekanisme, ti målinger totalt. Tabell 11 angir parametrene som er forskjellige. Testene med 802.11i med 802.1X ble gjennomført umiddelbart etterpå. Tabell 13 viser resultatene av målingene. Gjennomsnittet av alle målingene ble 21,2 Mbit/sek.

Tabell 13: Resultatene fra ti båndbreddemålinger med CCMP som sikkerhetsmekanisme

Forsøk	Tid	Overført	Throughput
1	10,0 sek	25,2 Mbyte	21,1 Mbit/sek
2	10,0 sek	24,1 Mbyte	20,2 Mbit/sek
3	10,0 sek	25,6 Mbyte	21,5 Mbit/sek
4	10,0 sek	25,3 Mbyte	21,2 Mbit/sek
5	10,0 sek	25,0 Mbyte	21,0 Mbit/sek
6	10,0 sek	25,7 Mbyte	21,6 Mbit/sek
7	10,0 sek	25,2 Mbyte	21,1 Mbit/sek
8	10,0 sek	25,4 Mbyte	21,3 Mbit/sek
9	10,0 sek	25,6 Mbyte	21,4 Mbit/sek
10	10,0 sek	25,4 Mbyte	21,3 Mbit/sek
Gjennomsnittlig		25,3 Mbyte	21,2 Mbit/sek

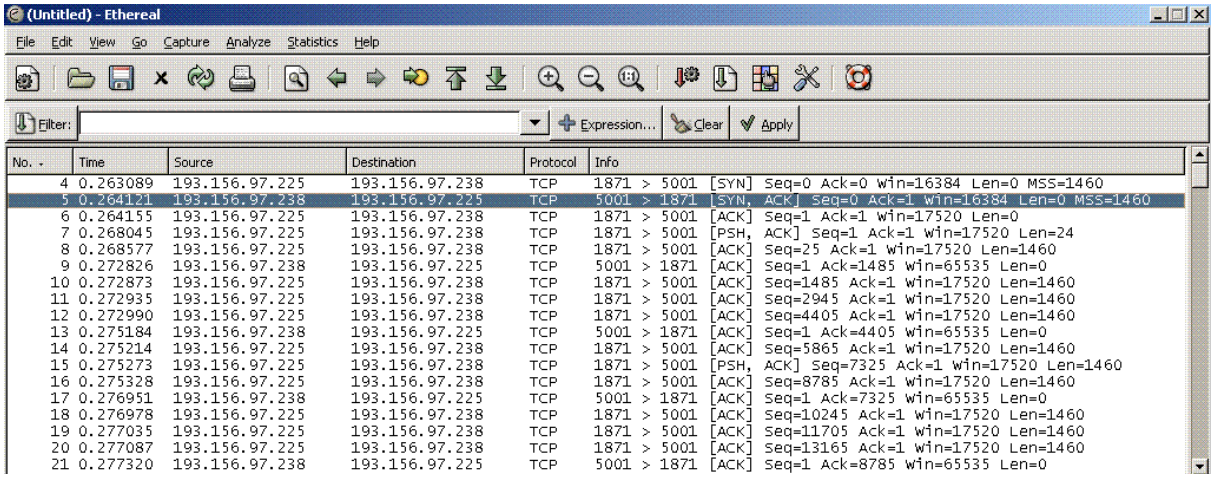
Alle målingene, totalt tjue, ligger ganske nære hverandre. Dersom de plottes inn en graf, vil det være enklere å se sammenhengen. Figur 16 viser en graf med alle tjue målingene.



Figur 16: Sammenligning av throughputmålinger

WEP-kryptering har ut i fra det som kan lese ut av grafen noe høyere throughput enn CCMP kryptering. Gjennomsnittlig throughput ved bruk av WEP som sikkerhetsmekanisme ble i dette forsøket 21,7 Mbit/sek. Den samme verdien for CCMP ble 21,2 Mbit/sek. 0,5 Mbit/sek økning fra 21,2 Mbit/sek til 21,7 Mbit/sek utgjør en økning på 2,4 %.
En økning kunne forventes ut i fra kjennskapen til at nyttetrafikken i en ramme som benytter WEP blir forholdsvis høyere enn nyttetrafikken i en ramme som benytter CCMP.

I kapittel 3.3 viste en utregning at throughput ikke burde endres med mer enn 0,5 % når WEP erstattes med CCMP dersom alle rammer som sendes i nettverket har 1500 byte nyttelast. Figur 17 viser de første 18 rammene som utveksels når Iperf benyttes til å måle performance. De samme innstillingene har blitt benyttet gjennom alle testene i hele denne oppgaven.



Figur 17: Noen av pakkene som utveksles under målinger med Iperf

I et praktisk tilfelle vil ikke alle rammene ha 1500 byte nyttelast, selv om pakkene settes opp til å ha maksimal størrelse 1500 byte. De aller fleste pakkene som sendes den veien dataene overføres vil ha størrelse 1500 byte. I en forbindelse vil det også sendes rammer tilbake uten nyttelast for å bekrefte mottak av mottatte rammer. Dette er en av årsakene til at forskjellen blir større enn teoretisk utregnet.

5.3 Se NRK.no Web-TV

Performance-testen avdekket at det var noe forskjell på throughput i IP-trafikk ved bruk av WEP og CCMP som krypteringsalgoritme. Den benyttet seg av Iperf for å måle throughput.

For å forsøke å finne ut om det kan oppleves noen forskjell ved å se direkteoverført video (streamet video) over de forbindelser som er kryptert ved hjelp av de WEP og CCMP skal denne testen gjennomføres. Testen tar ikke sikte på å beskrive annet enn eventuell forskjell i opplevd kvalitet. Det trådløse testnettverket kobles til UniKs nettverk for å få forbindelse til Internett. Figur 11 illustrerer denne konfigurasjonen. Den gjennomføres på den samme trådløse klienten. Som nettleser benyttes Microsoft Internet Explorer 6.0. Windows Media Player 10 benyttes som videodekoder.

Først gjennomføres testen over en forbindelse med WEP som sikkerhetsmekanisme, etterfulgt av et nytt gjennomløp med CCMP som sikkerhetsmekanisme. Testen gjennomføres ved at Internettleseren navigerer til http://www.nrk.no. Valget Nett-TV finnes i menyen til venstre. Et nytt nettleservindu åpner NRK Nett-TV. Dersom man ikke er registrert på forhånd gjennomgår man registreringsveiviseren. Om man har brukernavn og passord fra før kan man logge inn med det. Et program velges i menyen til venstre. Programmet starter. Etter å ha sett etter og hørt etter anomalier i bildet og lyden i et minutt konkluderes det med at det ikke har forekommet. Testen kjøres så på nytt igjen etter at forbindelsen er omstilt til CCMP. Det samme gjentar seg, uten anomalier.

Testen ble gjennomført med en strøm på 891 Kbit/sek, maksimalt oppnåelig. Hovedårsaken til at dette sannsynligvis ikke er en særlig god test er at Windows Media Player buffrer denne forbindelsen før den starter avspillingen. Ved å holde seg med en buffer opplever ikke brukeren variasjoner i throughput.

5.4 Sammendrag

Dette kapitlet har forklart forundersøkelsen, måling av throughput utført ved hjelp av Iperf og testen med streamet media. Forundersøkelsen viste at nettverkets konfigurasjon har mye å si for throughput. Testnettverket ble satt opp med kun et trådløst knutepunkt og en tjener tilknyttet en switch for ikke å få forstyrrelser fra UniKs nett. Throughputmålingene med Iperf viste at CCMP får noe lavere overføringshastighet enn WEP. I testnettet hadde den trådløse forbindelsen med pakkestørrelse på 1500 byte 2,4 % høyere throughput med WEP enn med CCMP. Å se NRK.no Web-TV ble også benyttet som en performancetest. Dette var ikke en god test, og sanntidsapplikasjoner som internettelefoni (Skype) eller videotelefoni (MSN Video) kunne vært benyttet i stedet.

6 Diskusjon

Dette kapitlet vil oppsummere oppgaven, og se på hvilke muligheter 802.11i gir. Først vil oppsett av testnett og forsøkene gjennomgås, etterfulgt av presentasjon av en case og hvordan denne kunne forbedres ved å innføre 802.11i.

6.1 Oppsett av testnett/oppgradering

Testnettet ble i utgangspunktet satt opp som en del av UniKs nettverk. Konfigurasjonen ble senere endret noe under forsøkene for å eliminere feilkilder. Oppgaven beskriver UniKs nettverk og forklarer hvordan det trådløse nettet kan oppgraders til 802.11i. Det er mer krevende å sette opp et nettverk med 802.11is CCMP til å sikre forbindelsen og 802.1X til brukerautentisering og nøkkelhåndtering enn å benytte WEP og delt nøkkel-autentisering. Når WEP benyttes angis det i knutepunktet og klienten at WEP skal benyttes og den forhåndsdelte nøkkelen angis. Ved CCMP og 802.1X må den som setter opp, eller oppgraderer, nettverket ta stilling til hvilken EAP-metode og RADIUS-tjener som skal benyttes, og sette opp og vedlikeholde en PKI-infrastruktur om man ønsker å bruke sertifikater til brukerautentisering. Mer kompleks infrastruktur og økte krav kan bli mer tungvint å administrere.

Fordelen med å oppgradere er at forbindelsen sikres med en sikkerhetsmekanisme som ikke inneholder noen av svakhetene til WEP, og autentisering kan foregå ved hjelp av en anerkjent standard uten svakheten til 802.11s opprinnelige autentiseringsmekanismer. Sikkerhetsnivået i det trådløse nettverket heves.

UniK kan ved å oppgradere dra nytte av eksisterende brukerkontoer slik at brukeren slipper å lære et nytt passord/nettverksnøkkel. Brukeren får kryptert sin forbindelse med en egen nøkkel, og ikke en gruppenøkkel som i WEP der alle som kjenner den felles nøkkelen de deler kan avlytte nettverkskommunikasjonen din. Ved å oppgradere og øke sikkerheten gjøres det vanskeligere å få tilgang til nettet, og risikoen for innbrudd reduseres. Det kan koste mye dersom for eksempel regnskapene endres eller personopplysninger lekker ut, om ikke mye i kroner og øre med i hvert fall i omdømme. Ved å innføre 802.11i og aktivere logging på RADIUS-tjeneren er det mulig å se hvem som har fått tilgang, og også blitt nektet tilgang. Dersom en angriper ønsker å endre loggen må han etter å ha brutt seg inn på nettet bryte seg inn på tjeneren.

Ved bruk av PEAP som EAP-metode i testnettet er det vist at brukeren ikke trenger å få mer og forholde seg til enn å skrive inn brukernavnet og passordet sitt i en passorddialog. Dersom brukernavnet og passordet brukeren bruker for å logge på Windows XP lokalt samsvarer med det som er registeret i brukerdatabasen som for eksempel Active Directory kan Windows automatisk logge på nettverket med dette.

I hvilken grad brukerne vil oppleve noen endring i performance vil diskuteres i neste underkapittel.

6.2 Forsøk

Gjennom forsøkene dokumentert i denne oppgaven er det forsøkt avdekket i hvilken grad performance påvirkes av oppgradering til 802.11i og utskifting av WEP med CCMP som sikkerhetsmekanisme. Det trådløse knutepunktet og tjeneren ble frakoblet UniKs nettverk og knyttet sammen på egen switch i forsøkene for å eliminere feilkilder i forbindelses med måling av performance.

I dette tilfelle ble Iperf benyttet for å måle throughput. Iperf sender datastrømmen i 1500 byte store pakker. Det ble målt gjennomsnittlig 2,4 % høyere throughput med WEP enn med CCMP. Dette bekrefter teorien om at CCMPs dobbelt så store overhead i forhold til WEP påvirker throughput. Årsaken til at throughput prosentvis ble 2,4 % antas å være at bl.a. at det sendes pakker i nettverket uten nyttelast også, slik at gjennomsnittlig throughput aldri blir som om alle pakker i nettet hadde 1500 byte nyttelast/data.

For nettverk med trafikk som sendes i forholdsvis store pakker blir overhead liten. I praksis ble overhead målt til ca 2,4 %, der alle pakker med 1500 byte størrelse ville gitt 0,5 % økning. Dersom nettverket overfører mye trafikk med små pakker blir overheaden veldig stor. Der alle pakker har størrelse 100 byte vil dette i teorien bli 7,4 %. Praktisk er det ikke mål i dette forsøket, men dersom samme størrelsesorden brukes kan resultatet bli ca 20 – 30 %.

De fleste trådløse brukerne i UniKs trådløse nettverk benytter nettverket til å lese websider, hente e-post overføre filer og benytter for det meste protokoller som overfører relativt store pakker. Dersom brukermønsteret endrer seg eller trafikken i nettverket øker bør det vurderes å øke kapasiteten ved å sette opp flere trådløse knutepunkt.

6.3 Hvordan kan dette anvendes

I dette underkapitlet skal vi se nærmere på et konkret tilfelle der man kunne anvendt 802.11i for å autentisere brukere og forbedre sikkerheten.

6.3.1 Anvendelsesområder

802.11i bør innføres slik at WEP kan erstattes med CCMP i alle trådløse nettverk som benytter kryptering. Dersom nettverket er lite og endring av brukere sjelden inntreffer kan man vurdere å benytte PSK (forhåndsdelt nøkkel) for å slippe å sette opp egen RADIUS-tjener.

Har organisasjonen kapasitet til å sette opp og drifte egen RADIUS-tjener bør dette vurderes. Autentisering og nøkkelhåndtering blir langt bedre enn manuell oppdatering av forhåndsdelte nøkler.

Organisasjoner og bedrifter som tilbyr alle sine trådløse tjenester, bør også benytte sikkerhetsmekanismer. Det vil gi brukerne trådløs beskyttelse. 802.11i bør benyttes slik at brukerne ikke deler en felles nøkkel og kan lese hverandres kommunikasjon. For eksempel tilbyr Peppes Pizza sine kunder gratis bruk av Internett i restauranten, men forbindelsen er ikke sikret.

I "HotSpots" bør også tilbydere tilby sikkerhet. Dersom 802.11i innføres med 802.1X autentisering kan dette by på utfordringer og forenklinger. Noen forenklinger kan være at ingen, verken legitime eller ubudne brukere, får tilgang til det trådløse nettverket før de er autentisert. Dersom det velges en EAP-metode som innebærer brukersertifikater og kanskje også maskinsertifikater må ikke bare brukernavn og passord distribueres på forhånd, men også sertifikater.

6.3.2 Telenor Mobil Trådløs Sone

Trådløs Sone fra Telenor Mobil er en tjeneste som benytter seg av 802.11 trådløse nett for å tilby kunden trådløs tilgang til Internett. Dette gir kunde langt høyere hastigheter enn det som kan oppnås i det ordinære mobilnettet basert på GSM og GPRS. Det gir også høyere hastigheter enn det som er mulig å oppnå i mobildatanettet UMTS. Løsningen benytter 802.11 konfigurert for teoretisk hastighet inn til knutepunktet på 11 Mbit/sek.

Telenor Mobil bygger ut Trådløs Sone over hele landet, bl.a. på de mest attraktive kurs- og konferansehotellene rundt om i landet, en del flyplasser, småbåthavner og Statoilstasjoner.

Kunden gis tilgang til tjenesten ved at det er inkludert i mobiltelefonabonnementet, man har tilgang gjennom andre abonnement eller man kan kjøpe ”skrapekort” på stedet.

Tjenesten fungerer på den måten at når kunden aktiverer sitt trådløse nettverkskort, kobler til det trådløse nettet ”Telenor Mobil Trådløs Sone”, og åpner en nettleser vil den automatisk åpne en påloggingsside. Her logger kunden inn med sitt mobilnummer, brukernavn eller skrapekortnummer og passord ettersom hvordan kunden har tilgang. Etter påloggingen kan en fritt benytte Internett.

En slik løsning innebærer ikke annet en slags tilgangskontroll. Det eneste den gjør er å hindre uautoriserte nettverkskort i å få tilgang. Løsningen innebærer ingen kryptering av forbindelsen. Den ligger åpen for alle som ønsker å lytte på den. Dette er ingen heldig situasjon. Mange brukere, spesielt brukere fra store bedrifter, har anledning til å sette opp f.eks. en VPN forbindelse til det stedet i internett de kommuniserer med eller via. Dette gir beskyttelse, men har man ikke muligheten til dette er det lett for f.eks. en inntrenger som sitter på gaten utenfor hotellet å avlytte internettrafikk.

Sikkerheten i en Trådløs Sone er begrenset. Telenor Mobil forteller kunden at de ikke har noen sikkerhetsmekanismer etter pålogging til tjenesten da internett i utgangspunktet er åpent og ubeskyttet[30]. Videre forteller de kunden at selve autentiseringsprosessen er sikret.

Å benytte argumentasjon slik som Telenor Mobil gjør her er som å argumentere mot bruk av WEP, i mangel av noe bedre, med begrunnelsen at den har kjente svakheter. Litt sikkerhet er

alltid bedre enn ingen sikkerhet. De bør krediteres for å gjøre kunden uttrykkelig oppmerksom på at løsningen ikke har noen sikkerhetsmekanismer.

Dersom Telenor Mobil hadde innført 802.11i og CCMP i sine trådløse soner, ville kunden fått sikret den trådløse forbindelsen og gjort det svært vanskelig, om ikke umulig, for en tredjeperson å avlytte den trådløse forbindelsen for f.eks. å snappe opp passord når en bruker henter e-posten sin. Denne oppgaven har benyttet UniKs nettverk for å vise hvordan dette kan gjøres.

Ved å innføre 802.11i med 802.1X autentisering ville Telenor også slippe en egen prosess for autentisering. En bruker, berettiget eller urettmessig, vil ikke få tilgang til den trådløse linken før autentiseringen er fullført. Dersom brukeren ønsker å sikre forbindelsen ut i Internett lenger enn til det trådløse knutepunktet må han fremdeles benytte VPN eller lignende.

7 Konklusjon og forslag til videre arbeid

I dette kapitlet vil det konkluderes og gis forslag til videre arbeid.

7.1 Konklusjon

Gjennom oppgaven er følgende problemstilling besvart:

Hvordan kan et nettverk oppgraderes fra WEP til CCMP med 802.11is tilhørende autentiseringsmekanisme?
Denne oppgaven har benyttet UniKs nettverk for å vise hvordan et nettverk kan oppgraderes. En konfigurasjon med egen IAS tjener uten forbindelse til UniKs brukerdatabase er benyttet for å vise oppsett av egen RADIUS-tjener. Ved idriftsettelse på UniK ville UniKs RADIUS-tjener benyttes, eller den oppsatte RADIUS-tjener ville fungere som videreformidler (proxy).

I hvilken grad påvirkes gjennomstrømningshastigheten (throughput) av IP-trafikk når WEP erstattes med CCMP for kryptering og 802.11is tilhørende autentiseringsmekanisme?
Gjennom tester utført og dokumentert i denne oppgaven er det påvist at throughput i et nettverk som krypteres med CCMP synker i forhold til om det hadde vært kryptert med WEP. I den utførte testen økte throughput gjennomsnittlig med 2,4 % når WEP ble benyttet i forhold til når CCMP ble benyttet. Dette skyldes at overhead ved bruk av CCMP er 16 byte mot WEPs 8 byte.

Og i hvilken grad kan brukeren oppfatte at WEP erstattes med CCMP for kryptering og 802.11is tilhørende autentiseringsmekanisme?
I det oppsatte testnettet kan brukeren merke at det går litt saktere ved overføring av store filer. Ved raske overføring vil ikke brukeren merke noe. Dersom en bruker benytter overføringsmetoder som innebærer overføring av små pakker, for eksempel VoIP, må det tas i betraktning at overhead forårsaket av krypteringen blir relativt mye større med CCMP enn med WEP.

7.2 Videre arbeid

For å studere brukernes oppfattelse av oppgradering til 802.11i med 802.1X autentisering foreslås det å gjennomføre en brukertilfredshetsundersøkelse etter at en oppgradering er gjennomført.

Det foreslås også en studie av hvordan 802.11i kan benyttes i et trådløst miljø som omfatter et nettverk med flere knutepunkter eventuelt også flere nettverk med flere knutepunkter. Trådløse Trondheim er et prosjekt som utvider NTNUs trådløse aksess til hele Trondheim sentrum. Det vil være interessant å se hvordan brukeradministrasjonen håndteres når flere

brukere fra forskjellige brukerdatabaser og flere knutepunkter skal benytte samme infrastruktur.

Som videre arbeid foreslås også en studie av innføring av 802.11i med 802.1X-autentisering i Telenor Mobil Trådløs Sone. Problemstillinger som hvordan man forflytter seg fra en lokasjon til en annen, hvordan flere sikkerhetstjenere synkroniseres samt hvordan forbindelsen kan sikres utover den trådløse forbindelsen og videre inn i Telenors nettverk ved hjelp av supplerende teknologier vil være interessante å jobbe videre med.

Referanser

[1] K. Hole, E. Dyrnes og P. Thorsheim, Securing Wi-Fi Networks, Computer, side 28-34, July 2005

[2] IEEE Std 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE, 1999

[3] IEEE Std 802.11i, Medium Access Control (MAC) Security Enhancements, IEEE, 2004

[4] G. Steen-Olsen og A. Stalheim, Innføring i Nettverk – Infrastruktur, IDG bøker, 1997

[5] E. Rescorla m.fl., The Secure HyperText Transfer Protocol, IETF RFC 2660, August 1999

[6] T. Dierks m.fl., The TLS Protocol Version 1.0, IETF RFC 2246, Januar 1999

[7] J. Walker, "Unsafe at any key size; an analysis of the WEP encapsulation", Tech. Rep. 03628E, IEEE 802.11 committee, Mars 2000 (http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip)

[8] IEEE Std 802.1X, Port-Based Network Access Control, IEEE, 2001

[9] ISO, Cyclic Redundacy Check 32, ISO 3309, 1993

[10] Paal E. Engelstad, Security in 802.11 WLAN: State of the art and future challenges, UniK kollokvium, Desember 2005

[11] A. Roos, A Class of Week Keys in the RC4 Stream Cipher, September 1995

[12] S. Flurer, I. Mantin og A. Shamir, Attack on RC4 and WEP, 2001

[13] N. Ferguson, Michael: An Improved MIC for 802.11 WEP, Januar 2002 (http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-020.zip)

[14] NIST, Advanced Engcryption Standard (AES), FIPS PUB, November 2001 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

[15] D. Whiting m.fl., Counter with CBC-MAC (CCM), IETF RFC 3610, September 2003

[16] C. Chaplin, E. Qi, H. Ptasinski, J. Walker, S. Li, 802.11i Overview, IEEE, Februar 2005 (http://www.drizzle.com/~aboba/IEEE/11-05-0123-01-0jtc-802-11i-overview.ppt)

[17] B. Aboba m.fl., Extensible Authentication Protocol (EAP), IETF RFC 3748, Juni 2004

[18] C. Rigney m.fl., Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865, Juni 2000

[19] L. Strand, 802.1X Port-Based Authentication HOWTO, 2004 (http://www.tldp.org/HOWTO/8021X-HOWTO/)

[20] J. Leira, IEEE 802.1X, April 2005 (http://www.uninett.no/wlan/8021x.html)

[21] Microsoft Corporation, The Advantages of Protected Extensible Authentication Protocol (PEAP): A standard Approach to User Authentication for IEEE 802.11 Wireless Network Access, Microsoft Corporation, Juli 2003

[22] L. Blunk, J. Vollbrecht, PPP Extensible Authentication Protocol (EAP), IETF RFC 2284, Mars 1998

[23] B. Aboba, D. Simon, PPP EAP TLS Authentication Protocol, IETF RFC 2716, Oktober 1999

[24] J. Wright, Weaknesses in LEAP Challenge/Response, Defcon, 2003 (http://home.jwu.edu/jwright/presentations/asleap-defcon.pdf)

[25] Microsoft, Internet Authentication Service, Microsoft Corporation, 2005 (http://www.microsoft.com/windowsserver2003/technologies/ias/default.mspx)

[26] Senter for informasjonssikring, Sikkerhetsmekanismer i trådløse nett, SIS, 25. april 2005

[27] T. Cooklev, Wireless Communication Standards, IEEE Press, 2004

[28] Microsoft Corporation, Knowledge base article 893357, Microsoft Corporation, Mai 2005 (http://support.microsoft.com/default.aspx?scid=kb;en-us;893357)

[29] White Paper, A detailed examination of the environmental and protocol parameters that affect 802.11g network performance, Proxim Corporation, 2003

[30] Telenor, Nyttig å vite om trådløs sone (WLAN), Telenor Mobil AS, 2005 (http://telenormobil.no/bedrift/tjenester/traadloesinternettsone/beskrivelse.do)

[31] TechNet, Interpreting IAS-formatted log files, Microsoft Corporation, 2005 (http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/f6322ae0-fb0a-4379-ad54-80bc62f78310.mspx)

[32] TechNet, Deployment of Secure 802.11 Networks Using Microsoft Windows, Microsoft Corporation, 2005 (http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/ed80211.mspx)

Appendiks A: Installasjon av Windows 2003 Server med IAS

RADIUS-tjeneren, Internet Authentication Service installeres på en Microsoft Windows 2003 Server Enterprise Edition. Installasjonen utføres ved at en evaluation edition av Microsoft Windows 2003 Server lastes ned fra Microsofts hjemmeside, brennes til CD og startes opp fra maskinen som skal benyttes. Velg en enkel og standard konfigurasjon ved å følge installasjonsveiviseren. Kjør Windows Update og hent de siste oppdateringene. Konfigurer automatiske oppdateringer til å laste ned og oppdatere hver dag kl 0300.

Innstaller Certificate Services:

1. Installer Certificate Services fra Kontrollpanelets ”Add/Remove programs”.
2. Følg veiviseren og angi informasjonen i de neste trinnene:
   CA Identifying Information:
   Common name for this CA: IAS
   Validity period: 1 year
3. Certificate database settings:
   Certificate database: C:\Windows\system32\CertLog
   Certificate database log: C:\Windows\system32\CertLog
   Store configuration information in a shared folder: C:\CAConfig
4. Installer sertifikat ved å gå til http://localhost/certsrv og velg Request certificate, så Advanced certificate request og til slutt Create and submit a request to this CA.
5. Under Identifying Information fylles inn informasjon om sertifikateier, velg Server Autentication Certificate, Create new key set og Microsoft RSA SChannel Cryptographic provider, nøkkellengde 1024, og “store certificate in the local computer certificate store”. De andre verdiene kan stå uendret. Velg Request Certificate.
6. Gå til Administrative Tools og Certification Authority. Under maskinnavnet (IAS) og mappen pending requests velg sertifikatet som venter og trykk Issue.
7. Gå tilbake til http://localhost/certsrv og velg denne gangen ”View the status of a pending certificate request”. Velg sertifikatet og trykk Install Certificate.

Kjør Active Directory Installation Wizard:

1. Create New Domain
2. Domain in a new forest.
3. Angi domene: Svendsk.local og tjener: Svendsk0

Opprett brukerkontoer:

1. Opprett en gruppe WirelessUsers og gi medlemmene Remote Access rettigheter.
2. Legg inn nødvendige brukere og gi medlemskap i gruppen.

Installer Internet Authentication Serivce:

1. Installerer Internet Authentication Service fra Kontrollpanelets “Add/Remove programs”. IAS finnes under “Networking services”
2. Åpne Internet Authentication Service
3. Høyreklikk Internet Authentication Service og velg Egenskaper.
4. Kryss av for å logge Rejected authentication requests og Successful authentication requests.
5. Under Ports sjekk at Authentication har port 1812,1645. Avslutt Egenskaper.
6. Velg Remote Access Logging. IAS logger autentiseringsinformasjon til en lokal fil angitt her.
7. Legg til knutepunktet som RADIUS klient ved å høyreklikke RADIUS Clients og velge New Client.
8. Angi et navn under Friendly name
9. Angi RADIUS som protokoll og trykk Next.
10. Angi IP-adressen til knutepunktet.
11. Angi testing123 som shared secret og trykk Ferdig.
12. Høyreklikk Remote Access Policy og velg New Remote Access Policy. Angi et Policy name, Access Metod til Wireless og velg gruppen WirelessUsers opprettet tidligere. Sett Authentication Method til Protected EAP.
13. Avslutt Internet Authentication Service

Appendiks B: Installasjon av nytt Orinoco AP-700

Fremgangsmåten for å konfigurere et Orinoco AP-700 er som følger:

1. Koble til strøm og nettverkskabel.
2. Installert medfølgende programvare på PC og start ScanTool. Velg nettverkskort. Fra listen kan det leses ut IP-adressen som knutepunktet har fått tildelt.
3. Åpne en nettside med IP-adressen som adressen. Tast inn passordet public.
4. Ved første gangs navigasjon til denne siden kommer det opp en Setup Wizard.
5. Veiledningen gir steg-for-steg muligheten til å legge inn bl.a. systemkonfigurasjon, velge IP-konfigurasjon, angi passord, velge driftsmodus og nettverksnavn.
6. Step 1: Inneholder informasjon om oppstarsveilederen. Velg ”Setup Wizard”.
7. Step 2 (System configuration): Skriv inn:
   Name: ORiNOCO-AP-700-5a-b5-27 (Behold gjeldene)
   Location: UniK 305
   Contact name: Kristian Svendsen
   Contact e-mail: svendsk@unik.no
   Contact Phone: +47 64844755
   Velg “Save & Next”
8. Step 3 (IP Configuration). Behold Dynamic. Velg “Save & Next”.
9. Step 4 (Password configuration): Skriv inn passord etterfulgt av “Save & Next”.
10. Step 5 (Wireless Interfaces Configuration). Operational mode: 802.11bg (Beholder gjeldene). Velg ”Save & Next. Network name: UNIK_Test
    Velg “Auto channel select” og Transmit rate: “Auto fallback” etterfulgt av Save & Next.
11. Step 6 (Summary). Et sammendrag av valgene vil vises.
12. De andre innstillingene som ikke er med i oppstartsveiledningen må endres etterpå.
13. Gå til Configure -> Interfaces -> Wireless -> Endre kanal til 11.
14. Gå til Configure -> SSID/VLAN/Security -> Security Profile -> Velg 1 og trykk Edit. Huk av for 802.11i Station og Trykk OK.
15. Gå til Configure -> Radius Profiles -> Velg 2 EAP Authentication og trykk Edit. Fyll inn IP-address 193.156.97.208 (IAS Server). Fyll inn Shared Secret og Confirm Shared Secret med testing123. Trykk OK.
16. Gå til Commands og Reboot knutepunktet.

Appendiks C: Konfigurasjon av trådløs klient (Windows XP)

Den trådløse klienten som benyttet i dette testnettet er en Fujitsu-Siemens Amilo Pro V2020 med Windows XP Professional. Det trådløse kortet er et Intel PRO/Wireless 2200BG med firmware 0.1.4.

1. For å sette opp 802.11i/WPA2 må man for Windows XP laste ned: http://www.microsoft.com/downloads/details.aspx?FamilyID=662bb74d-e7c1-48d6-95ee-1459234f4483&displaylang=no
2. Nedlasting av oppdateringen i punkt 1 gir støtte for WPA2. Artikkel http://support.microsoft.com/?id=893357 beskriver at dersom ikke driveren til nettverkskortet støtter WPA2 vil ikke listen ”Nettverksgodkjenning” under ”Tilknytning” i egenskapene til det trådløse nettet liste WPA2 eller WPA2-PSK.
3. For å oppdatere nettverkskortet Intel 2200BG besøk supportsidene på: http://www.intel.com/support/wireless/wlan/pro2200bg/ og finn veien til ny driver på: http://downloadfinder.intel.com/scripts-df-external/Detail_Desc.aspx?&DwnldID=9250&ProductID=1784
4. Kjøring den nedlastede filen og velg avansert installasjon. Velge kun oppdatering av driveren. Etter ferdig installasjon er WPA2 og WPA2-PSK synlig i listen.
5. Fra Egenskaper for Trådløs nettverkstilkobling velges Legg til... Skriv inn SSID (UNIK_Test) og velg Nettverksgodkjenning (WPA2), Datakryptering (AES), Under godkjenning aktiveres IEEE 802.1X-godkjenning med EAP-Type Beskyttet EAP (PEAP). Under detaljer fjernes krysset ”Bekreft rotsertifikat”. Etter å ha valgt Sikret passord velges konfigurer. Her velges at klienten ikke skal benytte seg automatisk av Windows-påloggingsnavnet og passordet for å gi brukeren anledning til å taste inn dette selv.
6. Når nettverket kobler til kommer det opp en passorddialog.